NOTE

This Microfiche meets the quality requirements of the American National Standard for Microfiche of Documents (ANSI PH5.9-1975). However, because of imperfections in the document from which it was made, it contains images that are illegible or difficult to read. The source document for this microfiche is the best copy that could be obtained prior to filming.

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

HEARINGS

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIALS

OF THE

COMMITTEE ON SCIENCE AND TECHNOLOGY U.S. HOUSE OF REPRESENTATIVES

NINETY-EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 26; OCTOBER 17, 24, 1983

[No. 46]

Printed for the use of the
Committee on Science and Technology

U.S. GOVERNMENT PRINTING OFFICE
28-715 O WASHINGTON : 1984

H701-19

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
GEORGE E. BROWN, Jr., California
JAMES H. SCHEUER, New York
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
ALBERT GORE, Jr., Tennessee
ROBERT A. YOUNG, Missouri
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
STAN LUNDINE, New York
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
MERVYN M. DYMALLY, California
PAUL SIMON, Illinois
NORMAN Y. MINETA, California
RICHARD J. DURBIN, Illinois
MICHAEL A. ANDREWS, Texas
BUDDY MacKAY, Florida
TIM VALENTINE, North Carolina
HARRY M. REID, Nevada
ROBERT G. TORRICELLI, New Jersey
FREDERICK C. BOUCHER, Virginia

LARRY WINN, Jr., Kansas
MANUEL LUJAN, Jr., New Mexico
ROBERT S. WALKER, Pennsylvania
WILLIAM CARNEY, New York
F. JAMES SENSENBRENNER, Jr., Wisconsin
JUDD GREGG, New Hampshire
RAYMOND J. McGRATH, New York
JOE SKEEN, New Mexico
CLAUDINE SCHNEIDER, Rhode Island
BILL LOWERY, California
ROD CHANDLER, Washington
HERBERT H. BATEMAN, Virginia
SHERWOOD L. BOEHLERT, New York
ALFRED A. McCANDLESS, California
TOM LEWIS, Florida

J. H. Poore, *Executive Director*
Robert C. Ketcham, *General Counsel*
Regina A. Davis, *Administrator*
David S. Jeffery, *Minority Staff Director*

Subcommittee on Transportation, Aviation and Materials

DAN GLICKMAN, Kansas, *Chairman*

ALBERT GORE, Jr., Tennessee
MERVYN M. DYMALLY, California
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MICHAEL A. ANDREWS, Texas

WILLIAM CARNEY, New York
SHERWOOD L. BOEHLERT, New York
ALFRED A. McCANDLESS, California

CONTENTS

WITNESSES

September 26, 1983:

Page
- Neal Patrick, Milwaukee, Wis., accompanied by Paul Piaskoski, Esq., counsel 14
- Jimmy McClary, division leader for operational security and safeguards division, Los Alamos National Laboratory, Los Alamos, N. Mex., accompanied by Dotty Camillo, group leader, communications and telecommunications group, Los Alamos National Laboratory, N. Mex 34
- Donn B. Parker, senior management systems consultant, Informations Systems Management Department, SRI International, Menlo Park, Calif., and Geoffrey S. Goodfellow, senior systems analyst, SRI International, Menlo Park, Calif 54
- Stephen T. Walker, president, Trusted Information Systems, Inc., Information Systems Telecommunications, Glenwood, Md 85

October 17, 1983:

- Joseph R. Wright, Jr., Deputy Director, Office of Management and Budget, accompanied by John P. McNicholas, Chief, Information Policy, Office of Management and Budget 102
- Warren Reed, Director, Information Management and Technology Division, U.S. General Accounting Office, accompanied by Walter L. Anderson, Senior Associate Director, Information Management and Technology Division, and Harold J. Podell, Group Director with Information Management and Technology Division 184
- John W. Lyons, Acting Director, National Bureau of Standards, and Dennis Branstad, Manager, Computer Integrity and Security Technology Group, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Department of Commerce 226
- Melville H. Klein, Director, DOD Computer Security Center, National Security Agency, U.S. Department of Defense, accompanied by Col. Roger R. Schell, Deputy Director, DOD Computer Security Center 269
- Floyd I. Clarke, Deputy Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, accompanied by Kier T. Boyd, Acting Assistant Director, Technical Services Division, Federal Bureau of Investigation, and Anthony J. Adamski, Jr., Chief, Financial Crimes Unit, Federal Bureau of Investigation 413
- Richard H. Shriver, Assistant Secretary of the Treasury, Electronic Systems and Information Technology, accompanied by Dr. Bob Conley, Deputy, Advanced Technology; Joe Bishop, Deputy, Programs and Resources Management; and Paul Trause, Inspector General, U.S. Treasury 422

October 24, 1983:

- Willis H. Ware, information systems, security, and privacy, the Rand Corp 446
- Jack L. Hancock, senior vice president, corporate strategy and systems, Wells Fargo Bank 477
- Julius Cohen, Director of Technology, Information Resource Management Department, Grumman Aerospace Corp 492
- Robert Morris, technical staff, Bell Telephone Laboratories, American Telephone & Telegraph Co 507
- Elmer I. Clegg, vice president, marketing, Federal Systems Division, Honeywell Information Systems, Inc., accompanied by James I Bolton, program director, Federal Systems Division, and Paul E. Flaherty, director, software engineering, Federal Systems Division 525

Appendix—Statement submitted for the record by IBM Corp 541

Statement submitted for the record by the Memorial Sloan-Kettering Cancer Center 545

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

MONDAY, SEPTEMBER 26, 1983

House of Representatives,
Committee on Science and Technology,
Subcommittee on Transportation,
Aviation and Materials,
Washington, D.C.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2318, Rayburn House Office Building, Hon. Dan Glickman (chairman of the subcommittee) presiding.

Mr. Glickman. Why don't we go ahead and begin this morning. I might mention to the audience, after all of the members have their chance for opening statements, then the lights will have to go off, and we are going to show about 4 minutes from the movie "War Games," which I think outlines the problem fairly clearly, and then we'll go into our witnesses.

Today the subcommittee will turn to one of those emerging technical and legal issues that is beginning to affect our society in a very broad way—computer and communications security and privacy.

Computers and the communications links that connect them are becoming more and more important to modern society. Banks, hospitals, schools, businesses of all kinds, and the military have assembled vast amounts of data on which they, and we, depend. In fact, the average citizen is probably unaware of the true extent that computers touch his daily life. Because computers are usually unseen, few of us, I suspect, are fully aware of their growth and importance.

Possibly for this reason we have also been largely unaware of the possibilities for the improper use of computers or access to the information they contain. In some cases, we have failed even to take the most elementary precaution, the electronic equivalent of locking the door.

Yet, as recent events have shown, whenever there is something of value, we must take steps to protect it.

First, there was the popular film "War Games" in which a youngster is able to penetrate the computers of the North American Defense Command and almost precipitates World War III. While this ultimate disaster is not likely possible, the film does illustrate, I am told, certain break-in methods that are factual.

Then there was the disclosure that a group of Milwaukee young people—known as the 414's—had, in fact, broken into computers all over the country. Among their victims were the Los Alamos National Laboratory, the Sloan-Kettering Cancer Center in New York, and the Security Pacific National Bank in Los Angeles.

And as we shall learn today, there is an entirely underground culture of people known as computer hackers who continuously try to defeat the security measures programed into modern computers.

Beyond this, computer systems are vulnerable to a variety of intentional and unintentional actions than can result in errors, interruption of service, or unauthorized access to and manipulation of confidential information.

To gain a better understanding of these threats and vulnerabilities, the subcommittee is today beginning an in-depth series of hearings that we hope will not only lead to such an understanding, but also will identify steps that need to be taken to prevent abuse of this rapidly growing technology.

We ask ourselves questions. We are in an era where we cannot live without computers. Now, of course, we must learn to live with them. But have we lost control? Have we created a monster? Are we, in effect, the modern-day Dr. Frankenstein? Do we have a technical problem or is there an ethical problem? And I suspect the answer is probably both. But the fact of the matter is that the hearing today will try to dramatize the problem and also deal with the ways to prevent it from becoming a national catastrophe.

Our first witnesses will include one of the Milwaukee 414's, one of their victims, and computer security experts who together can give a clear picture of the dimensions of this problem.

In later hearings—and there will be two more in October—we will hear from both Government and private sector witnesses about their specific problems in assuring privacy and security.

Before I call on Mr. Carney, I think the chairman of the full committee, Mr. Fuqua has an opening statement which will be included in the record at this point.

[The opening statement of Mr. Fuqua follows:]

OPENING STATEMENT

HONORABLE DON FUQUA, CHAIRMAN
COMMITTEE ON SCIENCE AND TECHNOLOGY

SEPTEMBER 26, 1983

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

I'D LIKE TO COMMEND MY COLLEAGUE, DAN GLICKMAN, FOR CALLING THESE HEARINGS. CLEARLY THE SUBJECT OF COMPUTER AND COMMUNICATIONS SECURITY IS AN IMPORTANT ONE, AND WILL BECOME EVEN MORE SO IN THE FUTURE.

YOU ONLY HAVE TO VISIT YOUR LOCAL SHOPPING MALL OR SCHOOL TO SEE THAT TODAY'S YOUNGSTERS ARE A COMPUTER GENERATION. THEY HAVE THE SAME KIND OF PASSION FOR COMPUTERS THAT THEIR PARENTS HAD FOR CARS WHEN THEY WERE GROWING UP.

SO, IT DOESN'T TAKE MUCH OF A PROJECTION TO FORECAST THE DAY WHEN WE WILL BE COMPLETELY COMFORTABLE WITH COMPUTERS AS AN INTEGRAL PART OF OUR DAILY LIVES -- JUST AS THE AUTOMOBILE IS TODAY. EXPERTS TELL US THAT THE DAY IS RAPIDLY APPROACHING WHEN EACH OF US WILL HAVE A COMPUTER IN OUR HOME TO HELP US WITH BANKING, SHOPPING, AND MANY OTHER TASKS. AND VIRTUALLY EVERY INSTITUTION IN OUR SOCIETY WILL LIKEWISE COME TO RELY ON THE POWER OF COMPUTERS.

AS THIS TECHNOLOGICAL REVOLUTION UNFOLDS, SO TOO WILL THE POSSIBILITIES FOR ABUSE. THEREFORE, IT IS PARTICULARLY APPROPRIATE THAT A SUBCOMMITTEE OF THE SCIENCE AND TECHNOLOGY COMMITTEE TAKE AN IN-DEPTH LOOK AT BOTH THE BENEFITS OF WIDESPREAD COMPUTERIZATION AND THE RISKS TO PRIVACY AND SECURITY.

SO, I WOULD JUST ADD A WORD OF WELCOME TO OUR WITNESSES TODAY AND SAY THAT I LOOK FORWARD TO A VERY INTERESTING AND, I HOPE, USEFUL SERIES OF HEARINGS.

Mr. Glickman. Now I'll call on the ranking member, Bill Carney.

Mr. Carney. Thank you, Mr. Chairman. I applaud you for calling a series of hearings on commuter and—computer and communications security privacy, and I look forward to the testimony of our distinguished witnesses.

I am particularly interested in hearing from Neal Patrick of the infamous 414 Gang, as well as the subsequent testimony of the computer experts who can tell us how to prevent these "War Games" types of break-in in the future.

I believe that few of us realize the impact of computer technology in our daily lives. Every time we fill out a credit card application, apply for a bank transaction card or a loan, our names, addresses, and financial data and employment status becomes part of a large information network that, without proper safeguards, can fall into the hands of computer hackers. In the past, these hackers have mischarged merchandise over the telephone by using intercepted credit card numbers, they've broken into telephone systems, thus charging up to thousands, or possibly millions of dollars worth of telephone time without paying for this.

Most companies are unwilling to talk about computer crime because they do not want to discuss their security vulnerabilities. In fact, I understand that it is not uncommon for companies who have been victims of computer crime to hire the criminal in order to prevent future break-ins.

Mr. Chairman, with the evolution of the personal computer and the growing communications network, it is time for this subcommittee to look hard at the issues associated with communications privacy and commuter—computer crimes.

I again commend you on calling for these hearings, and I look forward to the other two hearings which will complete the series.

Thank you, Mr. Chairman.

Mr. Glickman. Thank you, Mr. Carney.

Now I call on our colleague, Albert Gore, who I believe is also having hearings this week on issues related to computers, and who has had a great deal of interest in this subject matter.

Mr. Gore. Mr. Chairman, I don't have an opening statement. We're having hearings on the role of computers in education. And I congratulate you on these hearings, I am looking forward to our witnesses.

Mr. Glickman. I would now call on our colleague, Bill Nelson, who is on the full committee, and who has been interested in the issue, particularly as it relates to the criminal code and the violation of rights by computer.

Mr. Nelson. I thank you, Mr. Chairman.

I think what is taking place today, as has taken place in the Nation over the course, especially of the last several weeks, is to focus national attention on the problem. I am particularly grateful for this, having passed, as a member of the board of legislature 6 years ago, the first computer crimes law in the Nation. Some 20 States have followed suit.

And upon arriving here in the Congress 5 years ago, Mr. Chairman, I saw that there was no such law on the books in the Federal sphere of government. That is what H.R. 1092 addresses, is putting on the books and giving to prosecutors the adequate tools to go after this highly sophisticated type of crime that is not only apparent now, but will be increasingly all the more evident in the future as we computerize our society.

Now the long and short of it is that there is an inventiveness among computer operators that we do not want to stifle. And as we approach the problems evident in the computerization of society, we want to try to draft any legislative response without discouraging that inventiveness. At the same time, there is a great opportunity for harm done to society with the use of computers, harm to the national security, harm to the international security through the banking system, and that is something that we must address.

Mr. Chairman, presently Don Edwards has the computer crimes bill in his committee, in Judiciary. He is going to get that moving. It has taken it thus far—I have had the bill in for 3½ years, and it is now ready to move because the national need for this kind of legislation has been demonstrated.

And I thank you, Mr. Chairman, for—through the offices of your good committee, for additionally drawing attention to this need for legislation. Thank you.

Mr. GLICKMAN. Thank you. Thank you, Mr. Nelson.

Now I'd like to call on a distinguished member of the Interstate—the Energy and Commerce Committee, Mr. Ron Wyden from Oregon, whom also has had a great deal of interest in the issue.

Mr. WYDEN. Thank you very much, Mr. Chairman. I'll be brief, and I appreciate the chance to sit with you today.

I think what this country's seeing is the development of a new concept in lawbreaking. One of its most tragic and profound implications is that it attracts some of the brightest young people who seem to fail to recognize the ethical and moral implications of their actions.

For example, I'm convinced that very few, if any, of the young hackers across this country would ever think of knocking an elderly down on the street and taking her money. On the other hand, the possibility that by touching a few buttons on a computer system, that hacker might wipe out the same woman's retirement savings is very real. I think all of us in the Congress understand that this is a complicated subject, but I think there's some practical things we can do.

For example, I think that, whenever a school offers basic courses in computer instruction, those courses should contain an ethics component. At the very early levels, it could be simple, focusing just on the wrongdoing of taking another's possessions; at upper levels, it could focus on some of the specifics of program privacy.

I raise this point very briefly, Mr. Chairman, because I would suggest that no matter how many laws we pass, we cannot ban computer crime. What we can do is educate our citizens about the risk. That is the heart of crime prevention, reducing risk. And I would just suggest as we examine specific legislative proposals, that we keep that in mind.

The second and final point I make, Mr. Chairman, is that I would hope in the Congress we focus on those who are most vulnerable to computer crime. I've introduced the Small Business Computer Crime Prevention Act. It has passed the Small Business Subcommittee; it will go to the full committee early in October; and I would hope it would be on the floor early in October. And there are some very simple things we can do to assist people who are very vulnerable like small business.

For example, I'd like to see the Small Business Administration use its national toll-free line, something that's already in place, to assist small business, give them advice on how to reduce computer risk. Small businesses are very vulnerable because they can't, by their nature, limit access, which is what some of the larger businesses do. That's the kind of commonsense approach I would hope we take.

Finally, Mr. Chairman, let me just say that this strikes me as an other area where kids in Nikes are ahead of governmental experts in three-piece suits. And you see this in one subject after another. And I would hope now in the Congress, through the good work of my colleague, Mr. Nelson, Mr. Gore, and yourself, Mr. Carney and others, we'd finally now try to play some successful catchup ball.

And I thank the chairman for letting me sit in.

Mr. **GLICKMAN**. Thank you very much, Mr. Wyden.

We have a statement at this time from Hon. Tim Wirth, chairman of the Subcommittee on Telecommunications in the Commerce Committee, that will be included in the record at this point.

[The prepared statement of Mr. Wirth follows:]

Statement of

The Honorable Timothy E. Wirth

GOOD MORNING, AND THANK YOU VERY MUCH FOR INVITING ME TO APPEAR BEFORE YOU TODAY. THE ISSUE BEFORE THE SUBCOMMITTEE--COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY--ARE AMONG THE MOST IMPORTANT LONG TERM ISSUES FACING THE COUNTRY. YET LITTLE ATTENTION HAS BEEN PAID TO THEM THUS FAR.

WE ARE CONSTANTLY BEING REMINDED THAT OURS IS AN "INFORMATION ECONOMY". AT&T'S TELEVISION COMMERCIALS TELL US THAT WE'RE ENTERING THE "INFORMATION AGE" AND THE INVASION OF COMPUTERS INTO OUR DAILY LIVES PROVIDES DRAMATIC TESTIMONY TO THE REVOLUTION WE ARE WITNESSING. THE MANY BENEFITS OF THE COMPUTERIZATION OF OUR SOCIETY AND ECONOMY ARE THE SUBJECT OF MUCH DISCUSSION. SATELLITES HAVE BROUGHT INTERNATIONAL COMMUNICATIONS TO EVERY NATION OF THE WORLD. COSTS HAVE CONTINUALLY BEEN REDUCED. LONG DISTANCE NOW CONNECTS THE NATION THE WAY LOCAL SERVICE ONCE CONNECTED CITIES AND TOWNS.

COMPUTER-AIDED DESIGN AND MANUFACTURE ARE TRANSFORMING THE MANUFACTURING SECTOR OF OUR ECONOMY. SOPHISTICATED MARKETING TECHNIQUES AND MANAGEMENT SYSTEMS CONTRIBUTE TO THE COMPETITIVENESS OF OUR BASIC INDUSTRIES. ENTIRE NEW INDUSTRIES--SUCH AS THE DATA PROCESSING INDUSTRY--HAVE BEEN BORN AS THE RESULT OF THE TECHNOLOGICAL REVOLUTION WE'RE FACING.

ALL OF THESE ARE POSITIVE DEVELOPMENTS, AND WILL MEAN ECONOMIC GROWTH FOR OUR FUTURE.

BUT THERE IS A DARK SIDE TO THIS REVOLUTION AS WELL. AS THE ECONOMIC VALUE OF INFORMATION INCREASES, WE MUST DEVELOP THE SAFEGUARDS

FOR THAT INFORMATION THAT HAVE PROTECTED OUR PHYSICAL POSSESSIONS IN THE PAST. WE IGNORE COMPUTER AND COMMUNICATIONS PRIVACY AND SECURITY ISSUES AT OUR OWN PERIL. WE MUST RECOGNIZE THE BENEFITS THAT INCREASING ACCESS TO INFORMATION BRINGS US, BUT ALSO RECOGNIZE THAT IT IS SOMETHING OF A TWO-EDGED SWORD.

WE REALLY HAVEN'T GRAPPLED WITH THE IMPACT THAT THE COMPUTER AND COMMUNICATIONS REVOLUTION WILL HAVE ON OUR DAILY LIVES AND ON OUR ECONOMY. THE SUBCOMMITTEE THAT I CHAIR, ON TELECOMMUNICATIONS, CONSUMER PROTECTION AND FINANCE, HAS ATTEMPTED TO LOOK AT SOME OF THESE ISSUES. WE HAVE HELD HEARINGS ON RESTRICTIONS ON TRANS BORDER DATA FLOWS. WE HAVE ADDRESSED THE RESTRUCTURING OF THE TELECOMMUNICATIONS MARKETPLACE AND HAVE SOUGHT THE ADVICE OF CARRIERS AND USERS, COMSUMERS AND MULTI-NATIONALS, ON THE MANNER IN WHICH THE GOVERNMENT SHOULD TREAT THIS TECHNOLOGICAL REVOLUTION.

WHILE THE VARIOUS SUBCOMMITTES OF THE CONGRESS CAN TAKE A PIECEMEAL LOOK AT THESE ISSUES, WE LCAK AN OVERALL UNDERSTANDING OF WHAT IS HAPPENING IN OUR SOCIETY, OUR ECONOMY, AND HOW OUR LAWS NEED TO BE UPDATED TO DEAL WITH THOSE CHANGES.

YOUR EFFORTS HERE TODAY WILL CONTRIBUTE MUCH TO OUR UNDERSTANDING, AND I AM GRATEFUL FOR THE SUBCOMMITTEE'S INTEREST IN THESE ISSUES. PERHAPS THE COMBINATION OF THE RECENT "HACKERS" WHICH WERE EXPOSED IN MILWAUKEE, COUPLED WITH THE POPULAR MOVIE "WAR GAMES", WILL MOVE THIS DISCUSSION INTO THE PUBLIC EYE AND HELP TO FORCE DEBATE ON THE IMPLICATIONS OF THE CHANGES THAT ARE OCCURRING ACROSS THE COUNTRY.

BUT MY OWN SENSE IS THAT THIS IS NOT ENOUGH. WHAT IS NECESSARY, I THINK, IS THAT DECISION MAKERS IN THE PRIVATE SECTOR, IN STATE AND LOCAL GOVERNMENT, AND IN THE FEDERAL GOVERNMENT, HAVE A BETTER UNDERSTANDING OF THE ROLE OF INFORMATION IN OUR SOCIETY, AND OF THE IMPACT THAT THEIR DECISIONS WILL HAVE AS A RESULT OF THAT ALL-PERVASIVE ROLE. UNHAPPILY, MANY IN GOVERNMENT ARE NOT EQUIPPED TO DEAL WITH THOSE ISSUES TODAY. WE HAVE AN FCC WHICH IS ENTIRELY INSENSITIVE TO THESE CONCERNS, WHETHER IT IS ADDRESSING THE NETWORKS' CONTROL OVER WHAT WE SEE, OR INCREASING THE NETWORKS' CONTROL OVER THE NUMBER OF TELEVISION OUTLETS THEY CAN OWN ACROSS THE COUNTRY. CLEARLY THE DIVERSITY OF INFORMATION GOALS, THAT MANY OF US HOLD DEAR, ARE NOT A PRIORITY FOR THE "UNREGULATING" FCC.

THE RUSH TOWARDS "UNREGULATION" IS MORE THAN SLIGHTLY RELEVANT. SEVERAL YEARS AGO, THE FCC HANDED DOWN ITS FAMOUS "COMPUTER II" DECISION, IN WHICH IT ATTEMPTED TO DELINEATE BETWEEN BASIC SERVICES (WHICH WOULD CONTINUE TO BE REGULATED AS COMMON CARRIAGE) AND "ENHANCED SERVICES", WHICH ARE OUTSIDE OF THE DEFINITION OF COMMON CARRIER. THE NETWORK USED BY THE MILWAUKEE HACKERS, KNOWN AS TELENET, FALLS UNDER THE HEADING OF "ENHANCED SERVICES".

YET TITLE XVIII, THE CRIMINAL CODE, WHICH CONTAINS OUR WIRETAPPING PROHIBITIONS, REFERS ONLY TO COMMON CARRIERS, AS DEFINED IN THE CONNUMICATIONS ACT OF 1934. BY ITS DECISION TO DEREGULATE THE PROVISION OF ENHANCED SERVICES, AND PLACING THOSE SERVICES OUTSIDE OF THE SCOPE OF COMMON CARRIAGE, THE FCC MAY HAVE UNWITTINGLY MADE IT MORE DIFFICULT TO PROSECUTE THOSE WHO UTILIZE THOSE NETWORKS TO INVADE THE PRIVACY OF OTHERS.

THE PROBLEM IS ONLY GOING TO BECOME MORE ACUTE. IN THE FUTURE, OUR CARRIERS (BOTH COMMON AND OTHERWISE) WILL INCREASINGLY BECOME CUSTODIANS OF PERSONAL INFORMATION. THE ADVENT OF "VOICE MAIL", FOR EXAMPLE, IN WHICH THE CENTRAL SWITCHING SYSTEM BECOMES A COMMONLY-ACCESSED MAILBOX, WILL RAISE A HOST OF PRIVACY ISSUES THAT WE'RE GOING TO HAVE TO DEAL WITH.

OUR CURRENT LAWS ARE INADEQUATE TO DEAL WITH THESE ISSUES. TRADITIONALLY WE HAVE FOCUSED ON THE PRIVACY OF RECORDS: THOSE HELD BY THE GOVERNMENT, OR THOSE PERTAINING TO MEDICAL INFORMATION OR CREDIT INFORMATION, AND SO ON. THE NEW HOLDERS OF INFORMATION MAY NOT BE HOLDING RECORDS OF OUR PERSONAL LIVES, BUT MAY BE CUSTODIANS OF INFORMATION THAT IS FAR MORE VALUABLE.

WHAT IS TO BE DONE? WHERE DO WE GO FROM HERE? I WOULD SUGGEST THE FOLLOWING COURSE OF ACTION:

** WE SHOULD ENCOURAGE THE STATES TO CONTINUE TO DEVELOP THEIR OWN COMPUTER SECURITY STATUTES. CURRENTLY SOME 21 STATES HAVE LAWS ON THEIR BOOKS THAT DEAL WITH COMPUTER CRIME AND COMPUTER SECURITY. THAT IS A GOOD FIRST STEP, AND I WOULD HOPE THIS EFFORT WOULD SPREAD TO OTHER STATES. OUR LAWS MUST ATTACH TO THE INFORMATION ITSELF, RATHER THAN SIMPLY A RECORD SYSTEM CONTAINING INFORMATION.

BUT MORE IS NECESSARY.

** IN OUR EFFORTS TO BRING COMPUTER TECHNOLOGY INTO OUR SCHOOL SYSTEMS, WE SHOULD MAKE A DISCUSSION OF "COMPUTER ETHICS" AN

INTEGRAL PART OF THE CURRICULUM. THIS SEEMS ALMOST ELEMENTARY, YET I DON'T BELIEVE THAT WE HAVE FOCUSED ON IT IN THE PAST. JUST AS DRIVERS' EDUCATION HELPS TO EQUIP OUR NATION'S YOUNG PEOPLE TO BE SAFE AND RESPONSIBLE DRIVERS, SO SHOULD A COMPUTER ETHICS CURRICULUM EQUIP OUR YOUNG PEOPLE TO USE A COMPUTER RESPONSIBLY. CERTAINLY THE TOOLS OF THE COMPUTER AGE ARE AS POWERFUL AS THE AUTOMOBILE, AND SHOULD BE TREATED EQUALLY SERIOUSLY.

** AS A SOCIETY, WE NEED TO TAKE A LOOK AT THE LONG TERM IMPLICATIONS OF THE COMPUTERIZATION OF OUR ECONOMY AND OUR SOCIETY. I AM HESITANT TO SUGGEST THE FORMATION OF A NEW COMMISSION. BUT I DON'T KNOW WHAT OTHER APPROACH WE SHOULD TAKE. THE ISSUES INVOLVED IN THE COMPUTERIZATION OF OUR SOCIETY AND ECONOMY ARE OUTSIDE THE SCOPE OF WHAT WE'RE USED TO DEALING WITH. THEY ADD AN ENTIRELY NEW DIMENSION TO PUBLIC POLICY DEBATE.

WE LACK AN UNDERSTANDING OF THE CHALLENGES OUR SOCIETY WILL FACE, AND UNTIL WE HAVE A BASIC UNDERSTANDING OF THESE, WE CANNOT FORMULATE A RESPONSE.

WE HAVE A MODEL: THE PRIVACY COMMISSION, WHICH HELPED US TO UNDERSTAND SOME OF THE COMPONENTS OF THE COMPUTER REVOLUTION. BUT THE RECOMMENDATIONS OF THE PRIVACY COMMISSION HAVE LARGELY BEEN IMPLEMENTED. WE NEED TO PUSH OUR UNDERSTANDING OF THE FUNDAMENTAL CHANGES THAT ARE AFFECTING OUR SOCIETY BEFORE WE CAN ATTEMPT TO DEAL WITH THEM.

A "COMMISSION ON COMPUTER SECURITY AND CRIME" WOULD ASSIST

US IN GAINING THAT IMPORTANT UNDERSTANDING, AND I THINK WE SHOULD CONSIDER CONVENING SOME OF THE BEST MINDS IN THE NATION TO ADDRESS THESE ISSUES.

** THE PRIVATE SECTOR IS NOT WITHOUT A ROLE. I BELIEVE THAT ROLE IS SEVERALFOLD.

COMPUTER AND COMMUNICATIONS VENDORS MUST REALIZE THE COMMERCIAL VALUE OF SECURITY, AND BUILD IT INTO THEIR SYSTEMS. WHILE THIS IS ALREADY UNDERWAY IN SOME RESPECTS--DEFENSE COMMUNICATIONS, FOR EXAMPLE--FAR MORE IS NECESSARY, AS HAS BEEN SHOWN BY THE MILWAUKEE HACKERS.

IN ADDITION, THE PRIVATE SECTOR CANNOT HOPE FOR CONGRESS TO ENACT STATUTES THAT WILL PROTECT THEM FROM ABUSE WITHOUT THEIR PARTICIPATION IN THE LEGISLATIVE PROCESS. I UNDERSTAND THE RELUCTANCE OF BANKS AND OTHERS TO KEEP QUIET ABOUT VIOLATIONS OF THEIR COMPUTER SYSTEMS. NO ONE WANTS TO ANNOUNCE THAT THEY HAVE BEEN ROBBED OF THEIR DEPOSITS BY CRIMINALS MANIPULATING THEIR DATA PROCESSING SYSTEMS.

YET UNTIL THERE IS AN UNDERSTANDING OF THE MAGNITUDE OF THE PROBLEM, SOLUTIONS WILL CONTINUE TO BE ILLUSIVE. THUS, I BELIEVE THAT THE PRIVATE SECTOR MUST ASSIST US IN ASSEMBLING THE DATA NECESSARY TO RECOGNIZE THE SEVERITY OF THE PROBLEM, AND DEAL WITH IT IN A RESPONSIBLE FASHION.

MR. CHAIRMAN, I KNOW THAT YOU WILL BE RECEIVING A GOOD DEAL OF VALUABLE TESTIMONY ON THE PROBLEMS OF COMPUTER AND COMMUNICATIONS

SECURITY AND PRIVACY. I COMMEND YOU FOR CALLING THESE HEARINGS TODAY. I HOPE THAT MY CONTRIBUTION WILL ASSIST YOU IN YOUR EFFORTS, WHICH ARE OF TREMENDOUS IMPORTANCE.

THE DAWNING OF THE INFORMATION AGE WILL TRANSFORM OUR SOCIETY AS WE KNOW IT TODAY. BUT WE CANNOT PERMIT THE TECHNOLOGICAL REVOLUTION TO RUN ROUGHSHOD OVER THE RIGHTS AND PRIVLEGES OF OUR SOCIETY. THE DARKER SIDE OF THE COMPUTER AND COMMUNICATIONS REVOLUTION MAY MEAN AN INVASION OF OUR LIVES TO AN EXTENT UNDREAMED OF IN THE PAST. I THANK YOU FOR YOUR EFFORTS TODAY, AND LOOK FORWARD TO WORKING WITH YOU IN THE COMING MONTHS TO ADDRESS THIS IMPORTANT SET OF ISSUES.

THANK YOU VERY MUCH.

Mr. **Glickman**. At this stage, we are now going to show a brief segment of the film "War Games," and we are particularly grateful to the people at MGM/United Artists for providing this clip. If possible, could we dim the lights back there so we could show it.

I might say that this clip shows a scene in which the film's young star breaks into his school's computer for the purpose of changing his grade, a sequence I'm told is quite realistic in terms of what real hackers do.

Dim the lights.

[Film shown.]

Mr. **Glickman**. Get the lights here.

I realize some of you would like to see the whole movie, but we have other things to do.

Our first witness today is a real live hacker, I guess you'd call him, Neal Patrick from Milwaukee, Wis., accompanied by his attorney, Piaskoski—is that pretty close?

Mr. **Piaskoski**. That's correct.

Mr. **Glickman**. OK. Thank you.

Why don't you come on up to the desk. I don't believe that Mr. Patrick has any form of formal statement, so you may proceed as you deem appropriate.

We are most appreciative that you have been able to come here today. As you know, the subcommittee is really trying to determine from a technical point of view how serious the problem is and what can be done—can be done to protect the privacy and security of individual people, to have their records protected, as well as perhaps larger implications. So why don't you go ahead and proceed as you deem appropriate.

STATEMENT OF NEAL PATRICK, MILWAUKEE, WIS., ACCOMPANIED BY PAUL PIASKOSKI, ESQ., COUNSEL

Mr. PIASKOSKI. I just want to give a short introduction of Neal.

He is human. He is 17 years old. He is a senior at Rufus King High School in Milwaukee, which is a school for the college bound. He is a member of the National Honor Society. He was a participant in the 1983 U.S. Academic Decathlon. He was elected a member of the National Forensic League in 1981, with a degree of excellence. He's a National Merit Scholarship semifinalist. He is a bright kid.

He also, as you know—he and his group—have talked to a number of computers across the country, nationally and internationally, some of them in Canada, some on the east coast, some in the Southwest, some on the west coast.

Neal is not here today, though, as an information-age Robin Hood, as we've seen him called on occasion. He disdains that folk hero label, and probably the media attention, too.

He is here, I think, for the same reason that you've called this hearing. He's accepted the invitation so that he can let the public know, and especially other young computer hobbyists, that there are pitfalls, there are dangers, that there is potential harm that can be done, and that intellectual curiousity perhaps does not outweigh that risk.

Mr. GLICKMAN. Thank you.

Mr. Patrick, do you have any opening comments that you would like to make describing basically your background in computers and kind of giving some chronology of what happened, how you got involved in this situation, how you gained entry into other systems, perhaps providing a narrative background for us in your own words?

Mr. PATRICK. I don't—I don't have any opening statements, thank you.

Mr. GLICKMAN. OK. Well, if I could then ask you some opening questions, perhaps some background questions, and other members of the committee, I know, will, too.

Why don't you kind of give us an idea how you got interested in computers?

Mr. PATRICK. OK. At school, at Rufus King Middle School, there was a seventh grade 6-week course which was about a half an hour per day working with the Milwaukee Public Schools' computer. And in that we learned basic programing techniques and basic programing, and basically just learned about the computer. And that sparked my interest in computers.

Mr. GLICKMAN. And this was in the last couple of years?

Mr. PATRICK. Yes; it was.

Mr. GLICKMAN. OK.

What kind of computers were you learning on? Were they——

Mr. PATRICK. We learned on the computer that was provided by the Milwaukee Public Schools. It was a mainframe computer.

Mr. GLICKMAN. And you learned, would you say, elementary—basic elementary information about the use of computers?

Mr. PATRICK. Yes. That's all I learned at that time.

Mr. GLICKMAN. I assume they did not teach you how to break into other systems in the——

Mr. PATRICK. No.

Mr. GLICKMAN [continuing]. Milwaukee Public Schools.

Mr. PATRICK. No.

Mr. GLICKMAN. OK.

Now, were there friends of yours who also were associated with you in this instructional pattern? I mean, the group—the media's referred to the 414's. I assume that there was a group of friends of yours who were—who learned at the same time, became interested at the same time?

Mr. PATRICK. Not really. It was more just—it's comparable to a group of people who would get together to study, in that sense. We were all just happened to be interested in computers. The ages ranged—there was no other member of the group that attended my school, and we just got to know each other through the bulletin boards and through various conversations, and things of that sort, where we became interested in computers.

Mr. GLICKMAN. Did you then buy a home computer after your instructional course?

Mr. PATRICK. Yes. About 2 years after I received the course, we got our own computer.

Mr. GLICKMAN. What kind of computer was it?

Mr. PATRICK. It was a TRS-80, model II. It was basically for my father's business, but I ended up using it to learn basic—and learn various computer languages.

Mr. GLICKMAN. Between the time you took the course and you bought the computer, were you engaged in additional educational activities regarding the use of computers?

Mr. PATRICK. No.

Mr. GLICKMAN. So, really, then, your interest emanated, started up again, when you actually bought the computer, your father bought the computer?

Mr. PATRICK. Yes.

Mr. GLICKMAN. I have heard that many young people, interested in computers and accessing systems, communicate through electronic bulletin boards. Is that true, and can you describe what an electronic bulletin board is?

Mr. PATRICK. Well, that's sort of like saying people talk through the—you know, various—it's comparable just to talking through a telephone. Not everyone talks about the same thing, not all people on bulletin boards are interested in hacking, as they call it, but that's probably the best place to get information about accessing computers, because of the fact that everybody—or just about everybody—who uses bulletin boards is interested in computers in one way or another.

Mr. GLICKMAN. So what kind of information would you pick up from this bulletin board?

Mr. PATRICK. Various ways of accessing computers, such as passwords that could be tried. Default passwords are probably the easiest way of accessing computers because of the fact that every—or large numbers of computers around the country would have the same passwords because the system operators may not take out that time to change the passwords.

Mr. Glickman. So, theoretically, then, the bulletin board might say use this password because we find that it is a common password in this kind of computer system?

Mr. Patrick. Yes.

Mr. Glickman. Now, let me ask you this. When did you become active in the group called the 414's?

Mr. Patrick. The group got together, I'd say, about 6 to 8 months ago, and we had, you know, talked to each other about home computers and our interests sort of extended to the point where—where we wanted to do more than just play around on our home computers, and we got interested in using larger computers. And in that sense, we, you know, thought it might be interesting to try and access other computers.

Mr. Glickman. OK. So how did you do that then?

Mr. Patrick. We found out on a bulletin board system——

Mr. Glickman. I'm sorry. I didn't hear you.

Mr. Patrick. We found out on a bulletin board system the local telephone number of the local Telenet office, and just by calling that local number up, it hooked us up with a computer—a network of computers that could be accessed just by typing in five digits.

Mr. Glickman. Now tell me, what is a Telenet system?

Mr. Patrick. OK. What it is is a network—excuse me—a network of computers hooked up where you call up a local office and it connects you with a computer, and you plug in your modem and it connects you with the computer and, just by typing in five digits, it will connect you to computers all around the country.

Mr. Glickman. And will it describe the computers in detail so you'll know whose computer——

Mr. Patrick. No, it will not.

Mr. Glickman. It will not. So how will it—I mean, when you know you're hooked up to computers all over the country, how do you know that?

Mr. Patrick. OK. The five digits—you type in the first three digits are the area code of the place you want to call—for instance, 213, Los Angeles, and 312, Chicago—and the next two digits would be the—what they call the node numbers of those computers. And it's just like a line of computers hooked up to that Telenet network.

Mr. Glickman. So you would dial 312, that's the—what's the area code of Chicago.

Mr. Patrick. Yeah, 312.

Mr. Glickman. Three-one-two. And then you would dial two additional numbers, those were known numbers?

Mr. Patrick. Just, for instance, you type in 31223, and that might tell you that—it might say you connected to a computer, it might say that there is no computer on the other end of that line.

Mr. Glickman. So it would be essentially a trial-and-error method then?

Mr. Patrick. Right.

Mr. Glickman. So you just keep running through numbers until, whammo, something would appear on your screen which would indicate that you're actually into a computer system?

Mr. Patrick. Yes. It would connect you up with a computer and, at that time, you'd have to type in, you know, the various ways—

you type in maybe your name or something like that to access that computer. It would go through its own setup for access.

Mr. **Glickman**. Well, would you know in advance what the setup is for access, or would it describe that when you actually got into the computer?

Mr. **Patrick**. Some would describe how to access. Others, including the ones that we did, we accessed, would just give you one prompt and you were—and we knew beforehand what the—what we had to type in to access those computers.

Mr. **Glickman**. And you knew that from what, the electronic bulletin board?

Mr. **Patrick**. Right. It's—once again, that's those default passwords that were set up years ago by the company making that computer. And just as a Cadillac or something might have those digital locks on the door, these had the passwords on the computer. They were all the same. And it was up to the system operators to change those passwords once they got the computer installed.

Mr. **Glickman**. And they never did.

Mr. **Patrick**. Yes.

Mr. **Glickman**. That is what you are saying?

Mr. **Patrick**. Yes.

Mr. **Glickman**. If they had, in fact, changed those passwords, would it have been impossible for you to enter?

Mr. **Patrick**. Yes. For—because the passwords are up to thirty-two characters long, the number of passwords that could be chosen gets to the point where it would take a computer over 10 years to figure out the password. So, for having one computer trying to access another computer, it would take years.

Mr. **Glickman**. OK.

So using then the trial-and-error method, coupled with the electronic bulletin board, which is basically kind of a national data base for computers—computer information, I would assume, an unauth—I mean, places where you could enter—you were able to enter into several computer systems?

Mr. **Patrick**. Once again, let me clarify that bulletin boards are not just information upon accessing computers. They cover a wide range of subjects. So that putting them all in one category is——

Mr. **Glickman**. It would be like a classi—you would have a classified page, essentially, in a newspaper. You'd have all sorts of information about computers.

Mr. **Patrick**. On some of them, yes.

Mr. **Glickman**. Yeah. Who runs these bulletin boards?

Mr. **Patrick**. Just everyday people, people who have a computer and feel like—feel that they could contribute by having a bulletin board. I, myself, have a bulletin board that emphasizes various games that can be played on the computer.

Mr. **Glickman**. And is it free to access into one of these bulletin boards?

Mr. **Patrick**. Yes, it is.

Mr. **Glickman**. OK. Now, I'm curious—without taking too much time, because I want to get to some of the other people on the panel here—if you might give us a little bit of information about how you gained access to some of the more highly reported cases, the Sloan-Kettering Cancer Clinic, the Los Alamos case. I wonder if you might describe that.

Mr. Patrick. In all these cases, the passwords were generally the same. Just by typing—for instance, in the Los Alamos case, by typing in an easily known password, such as—everyday word, such as "test" or "system," you might gain access to Los Alamos and, in turn——

Mr. Glickman. Do you mean with the simple word "test" or "system"——

Mr. Patrick. Yes.

Mr. Glickman [continuing]. You could gain access to a laboratory with incredible defense capabilities?

Mr. Patrick. In fact, that, by typing in simple letters and codes that connected from members of the group with over 40 different computers that were connected up to Los Alamos which, in a sense, were part of their own subnetwork within the Los Alamos National Laboratory.

Mr. Glickman. So you not only got the wheel, you got the spokes of the wheel, into bunches of other computers as well, by typing in computer names that hadn't been changed in years?

Mr. Patrick. Right.

Mr. Glickman. OK.

Now, when you got into Los Alamos, I wonder if you could tell me what you found there?

Mr. Patrick. From what I understand, the members of the group who accessed that computer did not look for anything, so—you know, they weren't looking for any specific information, so they really didn't find anything.

I think, in this case, anyways, the fact that we were able to access it represents more the potential than the realized damage, because there was—especially in various cases—there was no damage, but the potential for damage was enormous.

Mr. Glickman. It's been said that there is no way to break in—there was a New York Times article on Sunday that said there's really no way to break into highly classified information, secret information. Is that—do you believe that's true?

Mr. Patrick. I think so. I would at least hope so, because especially the Defense Department, in various classified computers such as that, are not hooked up to the public Telenet network and—so they are not easily accessed, as opposed to something like a college or—in this case, it happened to be a developmental computer for a bank out in Los Angeles.

Mr. Glickman. Now, with respect to the Sloan-Kettering Cancer Clinic, was your access the same way?

Mr. Patrick. Yes, it was.

Mr. Glickman. And this was, in a sense, kind of an accidental access? You were dialing numbers and you got one that—I mean, were you looking for Sloan-Kettering?

Mr. Patrick. No, we were not. We have no idea—in fact, we had no idea which computers we accessed until sometimes when the news—when the press told us that we accessed them, or that the computer we accessed was Security Specific Bank or Los Alamos Nuclear Research Laboratory.

Mr. GLICKMAN. Now, when you went into the computers of Los Alamos, for example, did you—did you input anything in there that would have changed existing information in that computer?

Mr. PATRICK. No, not that I know of.

Mr. GLICKMAN. OK.

How about the cancer clinic? There was some discussion that their records were modified a bit.

Mr. PATRICK. I don't think any records were modified. From what I understand, there was access—accidental deletions, but once again, that more covers the potential than the realized damage because, from what I understand, patients' records were on there, and if someone with a sinister intent had accessed that, the damage could have run into the millions. That is just in dollar value, not including human lives.

Mr. GLICKMAN. I'm just going to ask one final question. Based upon what you know about access to the computers, it is indeed possible for great and extensive damage to be done to people's personal records as a result of sinister application of the technology you talked about?

Mr. PATRICK. I think it is. But also I think it's very easy to prevent that. There is no need for million-dollar security measures, but just commonsense ideas and attitudes would prevent most of this, if not all of this, from happening.

Mr. GLICKMAN. Like what? What are——

Mr. PATRICK. Change the passwords once. Once the computer's installed, change the passwords. Prevent leaks of security, for instance, from—it is—it's our understanding that this—the whole release of this press and the public release of the fact that members of our group accessed computers came from the Government people, or the employees down at Los Alamos. That, in a sense, shows the potential for leaks, security—breaches of security—that are easily closed up. But unless they are done, unless they are closed up, the potential's enormous.

Mr. GLICKMAN. Thank you.

Mr. Carney.

Mr. CARNEY. Thank you.

Mr. Patrick, how may people are in the so-called 414 group?

Mr. PATRICK. There are seven members.

Mr. CARNEY. And you say none of which went to your school? You met them through the computer?

Mr. PATRICK. Through the computers or some members. There was no strict formal leadership or any formal organization. Some members met each other through school, other members may have met each other through various organizations, computer organizations, such as user groups or something of that sort.

Mr. CARNEY. Can you tell one's basic capabilities on a computer by talking with them over the computer or watching what they do?

Mr. PATRICK. You can. The way the bulletin board systems are set up, they are set up just as a regular bulletin board on the wall. By taking on a message, you can leave a message for other people and talk to them and go into great detail about your knowledge and find out about their knowledge.

Mr. CARNEY. Would you say that the seven young men were more qualified at computers—I'm not saying at hacking or—but they had a good idea of the function of a computer and how you can work with the computer for maximum benefit? Or were they just average young men who have a computer in their possession?

Mr. PATRICK. I think they were above average in the sense that they knew about computers and they knew a little bit more about computers than the average home buyer. But I don't think they were—any members of the group were geniuses or anything of that sort. So I think it's—it's an above average, but not——

Mr. CARNEY. They shared a hobby of such——

Mr. PATRICK. Yeah.

Mr. CARNEY [continuing]. That you spend a lot of time on?

Mr. PATRICK. Yes, that's——

Mr. CARNEY. So you have that common ground.

Mr. PATRICK. Yes.

Mr. CARNEY. My next question is—and I'm going to ask you a couple of questions, and I hope you don't take it in the wrong way.

How were you exposed? How did people find out of the work that 414 did?

Mr. PATRICK. Which people? Are you talking about——

Mr. CARNEY. Well, how did it become public knowledge that this group of young men were so capable of—at accessing of computers?

Mr. PATRICK. What happened was, after we had talked with various members of the FBI and the Justice Department, there was a security——

Mr. CARNEY. Could you stop there and tell me why you were talking to the FBI and the Justice Department?

Mr. PATRICK. Because every member of the group felt that it was just as important to tell them what we did as——

Mr. CARNEY. In other words, you volunteered, you came forward?

Mr. PATRICK. What—OK, I think I should backtrack a little bit.

We were—the FBI visited us, and when they visited us, every member of the group was willing and gave them a large amount of information. After that, after we talked to the FBI and various officials, there was what you might call a security leak out of Los Alamos, and that the press got hold of from an "unidentified source" that——

Mr. CARNEY. We're used to those here.

Mr. PATRICK. But—yeah. And it came out of Los Alamos that there was a group of young people in Milwaukee accessing computers.

Mr. CARNEY. OK. So, in other words, one computer that you might have accessed, or one of the group had accessed, tripped, and had some type of defensive device that made the user of that computer aware that someone had accessed its computer.

Mr. PATRICK. Yeah.

Mr. CARNEY. Is that correct?

Mr. PATRICK. That's what I think it was.

Mr. CARNEY. And then it came backward——

Mr. PATRICK. Right.

Mr. CARNEY [continuing]. From that point. And then you, as hobbiest, probably were just having a whole bunch, I guess—I imagine. I could have seen——

Mr. PATRICK. Up—up until the fateful day.

Mr. CARNEY. Right. Well, I can understand that, but I can also understand you doing it and with no malice at that.

Let me ask you a question. Prior to that happening with this access, do you know of any groups that might have done this type of thing for financial benefit?

Mr. PATRICK. Not that I know of. I think that most of those groups would be unwilling to talk about what they did and how they did it. Most messages on the bulletin board were left by single people rather than groups.

Mr. CARNEY. Do you know of any professional groups as—in relationship to your being young men and students, do you know of any professional groups that try to gain access to computers——

Mr. PATRICK. Not that I know of.

Mr. CARNEY [continuing]. For gain, for any gain?

Mr. PATRICK. No.

Mr. CARNEY. Have you ever heard of Tap?

Mr. PATRICK. Yes, I have.

Mr. CARNEY. That's an organization, and it is my understanding they actually have bulletins, letters, and communications back and forth.

Mr. PATRICK. From what I understand, it's a—it's a newsletter put out from New York about every—you know, about electronics, is my understanding.

Mr. CARNEY. And let me—do you know how big that organization is?

Mr. PATRICK. No, I don't.

Mr. CARNEY. Is that primarily a hobbyist group?

Mr. PATRICK. I really don't know exactly to what extent their interest goes.

Mr. CARNEY. I'm curious about the passwords. You say that the companies have established certain passwords for when they sell that equipment——

Mr. PATRICK. Yes.

Mr. CARNEY [continuing]. To a person—or a user, I guess is a better term.

How did you get access to the passwords?

Mr. PATRICK. From what I understand, we picked them up off of various bulletin boards and just by leaving messages for various people.

Mr. CARNEY. There are so few that each company uses that you could——

Mr. PATRICK. Yeah. The number is approximately, from my understanding, the ones that we knew of were about four or five. And I don't know exactly how many others there are, but I think four to five is a good estimate of the number of passwords, or default passwords, that would be set up on a system.

Mr. CARNEY. How many hours a week were you doing this?

Mr. PATRICK. Let's see. Maybe about—over the summer anyways—maybe about 20 hours a week. It was something to do during the evening and late evening.

Mr. CARNEY. I have one question, and I don't mean to pretend I have a sense of humor, you must have had a heck of a phone bill, I would suggest.

Mr. PATRICK. Once—well, once again, it was—this ended up, the way it was set up, it was just a local call. We'd call up and we connect up with a computer right there.

Mr. CARNEY. In other words, someone's computer, no matter where it would be located, could be available on a local call?

Mr. PATRICK. Not everyone's computer, but the computers that were hooked up or connected to that Telenet net——

Mr. CARNEY. A company that had reason to have information either go to or from Milwaukee——

Mr. PATRICK. Right.

Mr. CARNEY [continuing]. Would be a company that you could dial into by simply doing the five-digit number.

Mr. PATRICK. Right.

Mr. CARNEY. Plus the access number in the beginning.

Mr. PATRICK. Yes.

Mr. CARNEY. How did you get the access number? Is that a common——

Mr. PATRICK. It's because, from what I understand, it's a public network, there's an 800 number that you could call just to find out your local Telenet number.

Mr. CARNEY. And you say that the group was together for about 7 months. Were you doing this prior to that, or did you just start doing it 7 months ago?

Mr. PATRICK. I just really started doing that just about that time.

Mr. CARNEY. I find that amazing.

I also, as an opinion, I—you know, I can fully appreciate what you did. And I would imagine that you're not unique with the young men and women around this country who are just trying to find out how much you can get out of a piece of computer equipment. And I am sure that you didn't feel that you were doing anything that was illegal. And I could see, again, a lot of people doing this. And I hope you don't think my questions are meant to indicate anything else.

My last question. You spent about 20 hours a week doing this. You've had some experience certainly. I don't know if that is a lot of experience compared to other young men and women. But you feel strongly that, with commonsense and with a little bit of application from the users, they could almost virtually eliminate access, outside access, to nondedicated computers?

Mr. PATRICK. Yes. All that it requires is those rudimentary steps.

Mr. CARNEY. And for the record, when you got into Los Alamos, you did not get into any type of computer that was dealing with any classified information, did you?

Mr. PATRICK. Not that I know of. But, once again, there were approximately 40—40 other computers that were hooked up directly to the Los Alamos computer that were accessed.

Mr. CARNEY. You don't have the capability of getting into a dedicated computer; is that correct?

Mr. PATRICK. No, I don't think so. I don't think we could get into a dedicated computer.

Mr. CARNEY. And my final question to you, young man, is what's the highest score you ever got on Pac Man?

Mr. PATRICK. I don't play it.

Mr. CARNEY. Thank you very much.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you.

Mr. Gore.

Mr. GORE. Thank you very much.

I find this fascinating. I—I note that you're obviously extremely bright.

Am I correct in assuming that—that kids that aren't necessarily in the top 1 percent in intelligence around the country, or whatever, are also capable of doing this with the technology that's now available; is that a fair assessment?

Mr. PATRICK. That's right. Any average—or even, if you want to call it that, below average—it's something that just about anybody could do.

Mr. GORE. It strikes me that a lot of the victims of—of the break-ins were careless in the—almost as if they were leaving the keys in a parked car with the doors unlocked. That kind of invites trouble. Do you think that analogy is an appropriate one?

Mr. PATRICK. I don't know. It's a—I think a more appropriate analogy would be that, you know, we—from our point of view, anyway—we walked up to a door and walked—and the sidewalk to a door invites somebody to walk up that sidewalk, the doorbell invites somebody to ring the doorbell, and ringing the doorbell, somebody answers the door.

In that case the computers answered the door. And that's exactly how we felt about it.

Mr. GORE. Well, you recognize now that what you and your friends did was wrong. But it seems to me that our country has to recognize that, as more information is stored on these computer systems, they have to be protected. And to use the analogy again, the door has to be locked so that people aren't invited to come on in and take whatever they want. Would you agree with that?

Mr. PATRICK. Yes. I think there has to be a good education of the people, both in the potential and the steps that have to be taken, as well as what they should not—should and should not do as computer users.

Mr. GORE. How exactly were you caught?

Mr. PATRICK. I really don't know. Because the matter is still under investigation, the FBI is not willing—FBI is not willing to reveal exactly how it traced our steps.

Mr. GORE. Well, you referred to unidentified sources earlier. One such source of information said that when you broke into the bank computer out in California—what bank was that? The——

Mr. PATRICK. Security Pacific.

Mr. GORE. The Security Pacific Bank—that they detected your first—did you do that more than once?

Mr. PATRICK. Yes.

Mr. GORE. Apparently, the first time you went into that bank's computer, it left a record. Does that make sense? You know so much more about it than we do.

Mr. PATRICK. Yes, it does.

Mr. GORE. OK.

Now, I'm told that, after your first entry, they set a trap for you, and the trap was designed to keep you plugged into their computer long enough for them to trace the call. And they baited the trap with a piece of cheese. And specifically the piece of cheese was a game called Star Trek. Do you remember playing a game called Star Trek *in the bank computer?*

Mr. PATRICK. Yes, I do.

Mr. GORE. For a good long while?

Mr. PATRICK. Yes, I do.

Mr. GORE. Well, so apparently, while you were playing that Star Trek game, the computer alerted somebody that you were in there, and the trap was sprung, and they traced your telephone call. And then—were you the first one that the FBI contacted?

Mr. PATRICK. No, I was not.

Mr. GORE. What did you guys think when the FBI started calling you?

Mr. PATRICK. Well, in my case, they knocked on my door——

Mr. GORE. Did your—did your——

Mr. PATRICK [continuing]. At 9 o'clock in the morning.

Mr. GORE. Did your father or your mother answer the door?

Mr. PATRICK. Neither. It was my little sister. Her and myself were the only ones that were at home.

Mr. GORE. And they wanted to talk to you—did they?

Mr. PATRICK. Yes, they did.

Mr. GORE. What did you think about that?

Mr. PATRICK. I was awestruck and a little—a little surprised in the sense that, at the time, we were just playing a game almost, and suddenly it—the reality strikes.

Mr. GORE. I guess you got onto the phone to some of your friends?

Mr. PATRICK. Yes.

Mr. GORE. And were—were they awestruck also?

Mr. PATRICK. Yeah, they were, and very surprised.

Mr. GORE. Well, you're—you're handling this whole thing with a great deal of maturity, and you've obviously got a bright future and not—and not the least of the reasons why is that you recognize that what you did was wrong. You seem to have it in perspective.

What are your plans? I know that's a personal question, but I am just curious what you hope to do.

Mr. PATRICK. I would like to go on to college and major in possibly computer science, computer technology, that sort of thing.

Mr. GORE. Now, you think that—going back to this analogy of locking the door—based on your experience, you think there are plenty of ways to do that; is that correct?

Mr. PATRICK. Plenty ways of locking the door and plenty of ways——

Mr. GORE. And preventing unauthorized access by people like you and your friends?

Mr. PATRICK. Yes, sir.

Mr. GORE. Now to put this in perspective, your—your unauthorized access always relied upon the telephone system to which many computers are hooked up; is that correct?

Mr. PATRICK. Yes.

Mr. GORE. In fact, your name, the 414 Club, comes from the area code in Milwaukee?

Mr. PATRICK. Yeah.

Mr. GORE. In fact, if you look closely at the problem of computer processing, there are many other access points, aside from the telephone system, that people using more sophisticated equipment, such as foreign governments or corporate espionage agents, people who really were very serious, with a lot of money, and dedicated to getting unauthorized access could gain it in a number of other ways.

Are you familiar with the—I suppose, since you have been involved in this. you've looked at the broader picture. Do you have any thoughts to share on that?

Mr. PATRICK. Well, from what I understand, the Wisconsin State Journal was one paper that walked into an office and found passwords lying on—you know, tacked to the bulletin board and lying on desks and things of that sort, which, in itself, shows, in a sense, how easy it is to access even computers that aren't hooked up to the telephone lines.

Mr. GORE. I am wondering, a lot of Members of Congress use computers for their correspondence and other tasks these days. Do you know of any hackers that have hooked up to Capitol Hill?

Mr. PATRICK. Not that I know of.

Mr. GORE. Well, I'm relieved by that, but not much, because I know that we probably have the same—same vulnerabilities up here as some of these other operations do.

Thank you very much for coming here.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you, Mr. Gore.

Mr. Nelson.

Mr. NELSON. Thank you, Mr. Chairman.

Good morning, Mr. Patrick.

As I said earlier, you have focused attention on the problem. I think, in that regard, you have performed a service for the country, because a great deal of the problem heretofore has been swept under the rug since institutions that may have been broken into, financial and otherwise, have not wanted to admit that there was a problem. And, therefore, in your hacking, you have indicated that, with relative ease, that you can get into these systems.

I think, in my information about some of the classified ability of protecting systems, that a lot of our defense systems that need those protections have those protections. And I don't think you would have been able to get into them.

But the fact is, now that you have focused the national attention on the problem of those that you did enter, it has certainly made everybody go back and change the passwords and other protective measures so that this will not be as easy to get into.

But there are the situations where people can get into. Let me describe one situation that occurred about 6 months ago. A former employee of the Federal Reserve System who, at that particular time, was employed by a brokerage house in New York City, and who had the access code to the Federal Reserve System computer, without authorization, used that access code, dialed in, and had information available which could help him and/or his employer dealing in the New York markets.

The way he was caught was that an alert supervisor on that particular day noticed that the computer had been accessed by a code of another employee who happened to be sick that particular day. And knowing that, then the fellow was quickly apprehended and he confessed. And the long and short of it is that there was another example of an unauthorized access of which the Nation's laws were ill-equipped to deal with. In this particular case, they used the interstate commerce over-the-wire existing laws. But had that former employee made the call from the District of Columbia to the Federal Reserve System's computers, also in the District of Columbia, the maximum penalty would have been a $100 fine.

So I want to thank you that you have focused the attention of the Nation on this potential for harm. Certainly that harm is very evident in our national banking system, where billions of dollars are transferred from one account to another account, billions of dollars are transferred from accounts in the international banking system, by computer. So you have focused that attention.

Now, let me just ask you, did you see the movie "War Games?"

Mr. PATRICK. Yes; I did.

Mr. NELSON. Was anything gleaned from that movie? Did that instigate you and/or your friends in the activities that you engaged in?

Mr. PATRICK. That didn't—excuse me. That didn't instigate us at all. We were—once again, we were doing this a few months before "War Games" came out, which was late May. And the only connection that there was between the movie and what we did was that Joshua was used as a few accounts on some of the computers we accessed.

Mr. GORE. It was?

Mr. NELSON. I'm sorry. Could you repeat that?

Mr. PATRICK. OK. What happened was, after accessing the computer, we added another account with the name "Joshua" which was used in the movie, just as another little game that we played.

Mr. NELSON. All right. I'll yield to the gentleman from Tennessee.

Mr. GORE. Oh, well, I was just curious. You're saying that you found that that—you added it as another what?

Mr. PATRICK. As another account. For instance, one account might be "system," where you type in——

Mr. GORE. When you say "account," do you mean you added it as another one of your short list of commonly-used access——

Mr. PATRICK. Yeah.

Mr. GORE. Passwords that you found frequently worked?

Mr. PATRICK. Yeah. It wasn't—it wasn't one that frequently worked; it was one that we used after we had accessed the system to remain—or to continue to have access.

Mr. GORE. Oh. So after you access the first time, you can—you could—you can establish your own access——

Mr. PATRICK. Right.

Mr. GORE [continuing]. Word after that?

Mr. PATRICK. Right.

Mr. GORE. OK.

Mr. NELSON. Was this on each of the computer systems——

Mr. PATRICK. I won't——

Mr. NELSON [continuing]. Or just one specific one?

Mr. PATRICK. This was on a number. I don't know—I don't think it was on every one, but it was on a number of them.

Mr. NELSON. OK.

Now, under previous questioning of the committee, you have indicated that you saw after the fact that what you had done was wrong and that you had come forth and, thus, the cooperation with the authorities.

At what point in this whole continuum of activity did you first question the ethical propriety of what you were doing?

Mr. PATRICK. Once the FBI knocked at my door.

Mr. NELSON. So it was——[Laughter.]

So it was not until that particular point, not until the FBI came, that there was any thought that what you were doing was unethical or illegal?

Mr. PATRICK. The only question that came to us was whether or not damage to a computer was, in that sense, unethical or simply illegal. And we felt that mere access was not, in that sense, illegal.

Mr. NELSON. And you say the question was raised in your mind, was damage illegal or unethical?

Mr. PATRICK. It wasn't even a question; it was a feeling that damage was unethical or illegal in that vein.

Mr. NELSON. Was there any damage done to any of those computers or their programs that you accessed?

Mr. PATRICK. In the Sloan-Kettering, there was a doctor's bills, where—whereas doctors would be billed for services or would be billed for the time that he used, that was, I think, a day or so that was accidently deleted.

Mr. NELSON. Did you know that at the time?

Mr. PATRICK. No.

Mr. NELSON. When did you find out that, in fact——

Mr. PATRICK. When the people at Sloan-Kettering let a message saying that there had been damage done to their computer.

Mr. NELSON. Did you know that that was a possibility at the time that you were accessing Sloan-Kettering?

Mr. PATRICK. Not at the time, no.

Mr. NELSON. Well, again, you have focused the attention of the Nation that, indeed, that damage can be done. And it would have been disastrous had certain very essential medical record been erased or altered. So you can see the implications in the future for what might happen there if a computer was—the records there were responsible for certain medical treatment in the future and they were altered. That could have very serious implications for individuals as well as institutions.

You said that you did not pay for any of the long-distance telephone calls because there were no long-distance calls?

Mr. PATRICK. That's right. There were no long-distance calls. It was just a local call to connect up with a computer.

Mr. GORE. Would my colleague yield?

Mr. NELSON. Certainly. I yield to the gentleman.

Mr. GORE. I'm told that you also got Sprint or MCI access codes by dialing the headquarters there and then doing random series of a few digit suffixes to get what were essentially credit card numbers; isn't that correct?

Mr. Patrick. From what I understand, that is—was easily possible and, in fact, was easily available.

Mr. Gore. And was done, wasn't it?

Mr. Patrick. Not that I know of, no. Not in our case.

Mr. Gore. Not by the 414's?

Mr. Patrick. Not in our case, no. Not that I know of.

Mr. Gore. Well, OK. Thank you.

Mr. Nelson. Mr. Chairman——

Mr. Glickman. May I just ask a question?

Mr. Nelson [continuing]. I have—sure.

Mr. Glickman. There was a Washington Post story of August 30, following along with the question about the calls, and I am reading: "One day in which he said was a typical instance, Patrick broke past computer security at Security Pacific National Bank in Los Angeles. Patrick did not intend to crack that particular computer. It was all pure chance. The break-in worked like this: Patrick called Telenet, hooked the system to his modem and waited for connection. Then he typed a 6-digit code of letters and numbers into his computer. The first digit was the letter 'C.' This told Telenet he wanted to make his call collect. He wanted the computer he was calling to accept the charges. Some do, some do not."

Is that a fair statement?

Mr. Patrick. OK, that—in a sense, that was a fair statement that that's what the "C" for a collect call means. But at the time, it was our understanding that you just type "C" to connect.

Mr. Glickman. OK.

Mr. Nelson. OK. I'd like to continue, Mr. Chairman.

When this bill on computer crime starts moving later this month or next month, I don't know if the chairman of that committee—of that Subcommittee in Judiciary is going to call you as a witness. But were he to call you, one of the questions that he would ask you—as we devise a law giving specific—in law, a specific new crime, computer crime, and how that's defined in the Federal jurisdiction, one of the things that we want to prevent is the stifle—stifling of inventiveness, as I mentioned earlier today. There's a certain inventiveness that ought to be there among computer operators.

Now, on the basis of your experience, that question would be, at what point do you think that your curiosity and inventiveness ought to be allowed to operate within a computer network system and when should it stop.

Mr. Patrick. I think once intentive—or malicious intent occurs, that's the dividing line between curiosity and destruction.

Mr. Nelson. A criminal intent or a malicious intent?

Mr. Patrick. Right.

Mr. Nelson. What about separate and apart from criminal intent that you access a computer and you do damage to that computer and/or the information stored in that computer—without the criminal intent? What do you think ought to be done there?

Mr. Patrick. It's hard to say. That's, you know, a case-by-case basis. The—there's a difference between, I think, between accessing and deleting files and accessing for destruction purposes. And I don't know exactly how the—I haven't looked at the bill, so I really wouldn't understand where the point comes between mere access and destructive intent.

Mr. **Nelson**. OK.

Do you have an opinion—for example, if, say, we have a computer operator who is putting certain information into a computer, if someone were to sit down in the place of that computer operator and put in wrong information that did damage to the users of that information, and they intended to so do that, would you agree that that is an intention to damage a particular computer or system?

Mr. **Patrick**. Yes; it is.

Mr. **Nelson**. OK.

Now, let's change the facts a little bit. Instead of the person sitting down and using the computer, instead, over here in the wire in-basket, they change the information that the computer operator puts into the system so that the same end result of damage to that system is done, but it is not done through the means of punching keys on a computer keyboard, rather it's changed by means of altering the information that is put through the computer operator into the system. Would you think that that would be the same kind of——

Mr. **Patrick**. If it's intentional, yes, it is.

Mr. **Nelson**. OK.

Thank you, Mr. Chairman.

Mr. **Glickman**. Mr. Wyden.

Mr. **Wyden**. Thank you very much, Mr. Chairman.

Mr. Patrick, it is very good to have you here. And I think one of the things that concerns committee members the most is that this is an area that has attracted some of the best and the brightest young people, and that in so many instances we're not talking about hardened criminals, but really the country's future.

I'd like to know how you and your friends felt when you got access to these systems. What kind of feeling—what was your reaction when you would penetrate these systems?

Mr. **Patrick**. For us, it was sort of an intellectual curiosity. And for us it was something to try and something to discover, just as somebody climbing a mountain would feel. And it was, I think, in our case anyways, it was more in that vein than anything else.

Mr. **Wyden**. Would you say that you and your friends felt it was one of the most exciting things you've ever done in your life?

Mr. **Patrick**. I don't know about one of the most exciting, but it was—I don't even know if you could say it was really exciting, but there was a small level of excitement there.

Mr. **Wyden**. You told the committee that you really got your start with computers in school. And I think you heard me say in my opening statement that I'd like to see schools start, where they had computer instruction programs, an ethics program to try to translate the real implications of these wrongful acts into some specifics.

Do you think that's a good idea? Do you think school systems with programs in computer instruction ought to build a real ethics component into them?

Mr. **Patrick**. I think that's an important position, but also there's a position—there's a case that can be made for better computer teachers, so that the computer teacher knows exactly what his students are doing, as opposed to a computer teacher, which is prevalent in a lot of schools today, where a teacher doesn't know exactly what his or her students are doing.

Mr. **Wyden**. Was there an ethics component in your computer instruction program?

Mr. **Patrick**. No; there wasn't.

Mr. **Wyden**. Well, then, let's talk about the area you mentioned, the quality of the classroom instruction. Do you feel your classroom instruction was at the level it should have been? I gather you feel a more superior teacher would have imparted to you some of these kinds of concerns that later came to befall you with FBI and law enforcement people at the door?

Mr. **Patrick**. Well, I think our school's been lucky in that we do have relatively good computer teachers. But, once again, many of them, no matter how good they are, may not know exactly what you are going. And at the time, which was in seventh grade, I had—it was an introductory course, and so the computer literacy ethics question did not come up.

Mr. **Wyden**. If you could suggest to the Congress just one thing, just one particular initiative that would reduce computer crime in this country, what would that be?

Mr. **Patrick**. Probably the easiest would be just to make sure those—somehow get the idea across to those system operators that, you know, setting up those rudimentary steps are very important to computer security.

Mr. **Wyden**. I very much appreciate your answer because, again, as you heard in my opening statement, I think education is going to be the key to reducing the risk of computer crime in this country. And I gather from your answer you agree with me. I don't think this Congress can pass a law that says there shalt be no more computer crime. And, I think, the fact is we could pass cratefuls of laws to reduce computer crime and, until we did the kind of thing that you mentioned—try to educate people as to rudimentary principles and reducing the risk—we wouldn't be able to deal with this problem successfully. And I very much appreciate your answer there, because I think education is just going to be the heart of—of dealing with this problem.

The only other question I had for you dealt with press coverage. There are a lot of Members of the U.S. Congress who would have like to have seen themselves on the cover of Newsweek magazine like your——

Mr. **Patrick**. I'm willing to trade places. [Laughter.]

Mr. **Wyden**. I was going to say that I had a feeling you would hope that it might come about in another sort of way.

But I wonder your reaction from the standpoint of whether this tremendous coverage from the press, a room full of cameras and whatnot, is this furthering an understanding of—of the problem? Do you think that the press is really focusing on what it should be in terms of trying to educate the American people about this new risk?

Mr. **Patrick**. I would certainly hope so. I think that, generally, the press has been trying to get the idea across that some of these steps could have been taken, should have been taken, and, unless those steps are taken, the potential is enormous.

Mr. WYDEN. I wish we could have had you at our Small Business hearings. I've been particularly interested in the problems of small business. That's where 80 percent of the jobs are in this country. And I think that you and I would agree that the larger businesses have the expertise to deal with some of the computer risks, but small businesses really could be wiped out overnight and really not wake up until it's too late.

Do you think there should be more focus, both in the press and in the Congress, on these kinds of violations? They may not be Sloan-Kettering or sensational kinds of problems, but they're the garden variety kind of everyday occurrences that can mean so much to the well-being of our economy. Do you think we should be focusing more on those kinds of problems, small business and others?

Mr. PATRICK. Well, I think what we did not necessarily concern small businesses. But I think the—like you said, the potential for, you know, a business being wiped out overnight is definitely there, and it is definitely there if someone, say, comes in and says, "Well, let's see how this disk will do if I put a magnet up to it," or something like that. And there are, even in the case of small businesses, there are a few steps that should be taken where business or a business' livelihood is at stake.

Mr. WYDEN. I gather you and your friends really weren't in it for money, though.

Mr. PATRICK. No; we weren't.

Mr. WYDEN. Do you get the feeling that some people are, though? I mean, that's one of my concerns about small business. In particular, there, there's a chance to make—you know, if you wipe out somebody's accounts receivable, there's a chance to make a lot of money very quickly. And I gather from you that you are—your thrill of it all was the intellectual curiosity. But for a lot of other people, there's a concern that there's really some bucks to be made. There's this old Willie Sutton quote I'm sure you have seen, "Why did you rob a bank? That's where the money is." And why you rob the computer today? In effect, that's where the dollars are. I'm interested in your reaction to that.

Mr. PATRICK. Yeah. If—let's say a person decides to go into an accounting office and pick up their disks and use them for his own purposes. He can pick up, I'm sure, thousands of dollars worth of business just by finding out what's on those disks. And, yes, the need is there.

Mr. WYDEN. And we were lucky that in your case and your friends', there was intellectual curiosity. But in a lot of other cases, you'd just be going for the dollar signs.

Mr. PATRICK. Yes.

Mr. WYDEN. Mr. Chairman, I would just conclude with one observation. I thank Mr. Patrick. I think he has emphasized how important the educational functions are going to be in the school systems with the small business community and other sectors of the economy if we're going to reduce computer crime. I think we may need some new laws. But I would just suggest to my colleagues that we could pass laws until we literally ran out of paper on which to print them, but until we educated the American people about this new concept of lawbreaking, I think we'll have a little of difficulty significantly reducing its incidence.

I thank the Chairman.

Mr. GLICKMAN. Thank you.

I think that Mr. Carney has two quick questions.

Mr. CARNEY. Mr. Patrick, if you don't want to answer this question, you don't have to, and if your counsel suggest not to. But it has nothing to do with you personally. But in general, I'm under the impression that accessing a computer is not illegal; is that correct?

Mr. PATRICK. It depends. You know, it was our impression before this that it was not. But it is our understanding now that it is, even—I don't know. Maybe you could quote him more detail about the actual laws.

Mr. PIASKOSKI. There—there are a number of States that have computer access laws. Wisconsin is one of them. It does make access of a computer unauthorized access, a crime running anywhere form a misdemeanor to a serious felony, depending upon whether you've done damage and how much damage you've done.

Mr. CARNEY. Let me ask you a question along those lines.

Isn't it possible for you to access a computer by mistake?

Mr. PATRICK. Yes, it is. It definitely is.

Mr. CARNEY. I mean——

Mr. PATRICK. I think, after reading the State statute, I think the intent there, you have to—the State must prove the criminal intent of accessing.

Mr. CARNEY. But accessing a computer is—by mistake is as simple as dialing a wrong number; is that not correct?

Mr. PATRICK. Right. That's right.

Mr. CARNEY. So we'd have a very difficult time in establishing law to deal with access. You have to have proof of intent and that type of thing.

Mr. PATRICK. Yeah. I think proof of intent would have to be there.

Mr. CARNEY. One of the points I was trying to make, I think, and I think my colleague, Mr. Wyden, in his conclusion made that same point, and that is that perhaps we all recognize the importance of making the public aware of the fact that computers can be very easily accessed. But I think what we're trying to establish is how to prevent that. And it seems to me from just talking to you—and we have a wealth of other witnesses, and there are other subcommittees hearing this—that perhaps it's not so much Government's role to come out, spend an enormous amount of money trying to prevent this type of thing, or to promulgate an enormous amount of rules and regulations in public law, but a little bit of commonsense on the user can very well be the best way to prevent this type of access.

And the type of access we're talking about is a limited access to computers that use the telecommunications networks around our country that everyone has access to by the simple use of a telephone instrument.

We won 10—as businesses, and I agree small business cannot afford to have dedicated computers in many instances. But businesses dealing with propriety information and that type of thing can simply have dedicated computers. Business dealing with defense or security matters do have dedicated computers. And if we have done anything, we've created a public service or have done a public service by alerting everybody the simple access to these everyday home computers and computers that use the telecommunications line.

I think that might be the greatest role we, as a Government, can do. Now, a little bit of commonsense on the part of the user can prevent this thing from happening to the extent that it has. Would you not agree with that?

Mr. PATRICK. Yes, I would.

Mr. CARNEY. Thank you.

And, Mr. Chairman, I yield back the balance of my time.

Mr. GLICKMAN. Just two quick questions, Mr. Patrick.

Did Sloan-Kettering, the Cancer Clinic, try to communicate with you when you tried to get access to their——

Mr. PATRICK. Do you mean me personally, or a member of the group?

Mr. GLICKMAN. Well, with a member of the group.

Mr. PATRICK. Yeah. As I remember, after the system was accessed, a member of Sloan-Kettering did communicate with a member of the group.

Mr. GLICKMAN. And what—tell me what they said.

Mr. PATRICK. They discussed—a person at Sloan-Kettering discussed the damage and the potential for damage, and offered a demonstration account, which the member of the group accepted. And after that—at that point and after that point, only the demonstration account was used.

Mr. GLICKMAN. OK. So, essentially, Sloan-Kettering said something like please don't tamper with this computer, you may be interfering with human lives, we'll give you some unrelated time.

Mr. PATRICK. Right.

Mr. GLICKMAN. And this, itself, was the computer that had been programed to do this, so they were—I mean, was this a computer talking to another computer?

Mr. PATRICK. No.

Mr. GLICKMAN. Or was it a human being at Sloan-Kettering?

Mr. PATRICK. It was a human being at Sloan-Kettering talking to a member of the group over the telephone.

Mr. GLICKMAN. OK. So, apparently, their computer had enough sophisticated security into it to be able to ring a bell or to do something to be able to get the computer operator to come to the screen?

Mr. PATRICK. I don't know. Maybe the computer operator noticed that somebody was using the computer at, you know, 2 o'clock in the morning.

Mr. GLICKMAN. OK.

Let me ask you this. You know, a lot of people are interested. Do you believe that individuals, their bank accounts, their Master Charge accounts, their VISA accounts are safe today from computer intrusion?

Mr. PATRICK. I think they're safe from outside intrusion, but inside intrusion, they are probably very vulnerable.

Mr. GLICKMAN. So they are reasonably safe from hackers coming in from the outside.

Mr. PATRICK. Right.

Mr. GLICKMAN. But manipulators of the system internally they are not safe from.

Mr. PATRICK. Right.

Mr. GLICKMAN. Well, I want to thank you very much. You are a very—as Mr. Gore said—mature person who dealt with us today as well as any witnesses we have had before. And I know that you have been through a lot. And unrelated to either the legal or ethical implications, you have raised a subject matter which is critical to the effective functioning of our society.

You know, we're in an era where we cannot live without computers. Now we have to learn with them. And I think that your testimony today will help us, help the private sector, help the Government, learn to live with computers.

So we are appreciative that you came here today, and we thank you very much.

Mr. PATRICK. Thank you.

Mr. GLICKMAN. We have as our next witness, Jimmy McClary, division leader for operational security and safeguards division of Los Alamos National Laboratory; and Mr. McClary is accompanied by Dotty Camillo, group leader, communications and telecommunications group.

We are appreciative that you are here. Do you have a statement?

Mr. McCLARY. Yes, Mr. Chairman, I do.

Mr. GLICKMAN. OK. Why don't you go ahead and proceed. You can either read it or you can summarize it, as you deem appropriate.

Mr. McCLARY. If you don't mind, I would prefer to read it.

Mr. GLICKMAN. OK, go ahead.

STATEMENT OF JIMMY McCLARY, DIVISION LEADER FOR OPERATIONAL SECURITY AND SAFEGUARDS DIVISION, LOS ALAMOS NATIONAL LABORATORY, LOS ALAMOS, N. MEX., ACCOMPANIED BY DOTTY CAMILLO, GROUP LEADER, COMMUNICATIONS AND TELECOMMUNICATIONS GROUP, LOS ALAMOS NATIONAL LABORATORY, NEW MEXICO

Mr. McCLARY. Mr. Chairman, I am Jim McClary, division leader of the operational security and safeguards division at the Los Alamos National Laboratory. With me is Dorothy Camillo, group leader of the computer and telecommunications security group at Los Alamos. The operational security and safeguards division has the responsibility for establishing and maintaining security at Los Alamos. The computer and telecommunications security group within the division has the responsibility for those specific aspects of security at the laboratory.

I wish to thank you for the opportunity to come here today to discuss the incidents involving unauthorized accesses by the so-called 414's to the open computers at the laboratory. I plan to discuss the security in the Los Alamos integrated computing network, the 414 incidents of unauthorized access, and the laboratory's response to these incidents. We will also discuss some conclusions we have drawn from these events.

At the outset, Mr. Chairman, I would like to emphasize that the computers involved in this incident are not used to process classified or sensitive unclassified information. Therefore, this incident involved no compromise of such information. It did consume the time of the system managers, security personnel, and definitely our public affairs office. In a moment, I will discuss the intrusions. But first, I will describe the basic security structure of our computing network at Los Alamos.

The laboratory's integrated computing network processes data of a wide range of sensitivities on many different types of computer systems. Because of the difference in data sensitivities, which range from unclassified scientific information to secret restricted data related to the design of nuclear weapons, and because of the diverse user population, we place a strong emphasis on matching the level of protection in a system to the sensitivity of the data.

At Los Alamos, we place computer systems into one of three categories, based on the sensitivity of the data processed. In the integrated computing network, these categories, or partitions, are referred to as the open partition, the administrative partition, and the secure partition. The incident being discussed today occurred at the periphery of the open partition.

The secure partition is the only part of the integrated computing network where classified data is processed. Users of the security partition must be Q cleared and authorized for access to this partition by their management. They must be—they must be located at physically protected terminals communicating over a protected distribution system, and must submit a password which is itself classified in order to do the classified work. Terminals authorized only for the administrative or open partitions of the network are not allowed to access computers in the secure partition. There is no dial-up access to the secure partition.

The administrative partition is used to process sensitive and classified data such as financial information, and data subject to the protection of Federal or State Privacy Acts. Users of this partition are laboratory employees who have obtained specific management authorization. There is no dial-up access to this partition either.

In the open partition, we allow only work which is unclassified and is not administratively sensitive. The authorized users of this partition are laboratory employees and others who have legitimate reasons for computing at Los Alamos and have contractual agreements with the laboratory. A typical nonlaboratory employee might be—user might be an employee of a laboratory subcontractor, a university faculty member, or an employee of some other DOE prime contractor. Dial-up access is provided for computers in this partition, and the users need not be cleared.

Although this partition is called open, it does not mean that the substantial computing resources available are unprotected or available to everyone. Each user of the integrated computing network is assigned a unique identification number and sign-on password. All passwords are issued by the computer security group. They are randomly generated and changed at least yearly.

Every attempt to sign on to the network requires that the user submit his or her unique identification number and password. These are checked by a separate computer called the network security controller. If they are correct, the user is allowed to access computers which he or she can run their own programs. Five incorrect attempts to supply a password are allowed. After five failures, the identification number is locked out until a security officer has taken action to allow the user to try again.

In addition to these main partitions, each of the three network partitions has a gateway computer which allows authorized organizations to connect their own Digital Equipment Corp. VAX computers to the partition. These computers, called distributed processors, are operated and maintained by the user organizations. Within the open partition, systems managers of the distributed processors are responsible for authorizing people to use their system, for control of passwards, and for monitoring usage of the system. They are constrained by DOE requirements, which implement OMB circular A71, that the system be used only for official business. However, a standard ICN and user number and password are required to make use of the gateway to the main body of the network.

Telenet is connected to one of these open partition distributed processors. This computer, referred to as machine G, was the one initially accessed by the youths from Milwaukee. In the following discussion, the computers in question are the distributed processors attached to the open partition of our network.

Late on June 28, 1983, the system manager for machine G discovered an unauthorized activity under a privileged account. He immediately reported it to computing division personnel who, in turn, notified computer security. Investigation showed that the intruder accessed machine G through its Telenet link. Telenet customer service was notified and their personnel traced the call.

I was notified by Telenet the next morning that similar activities from this number were currently under investigation by the FBI. Further checks of our records revealed that the intruder had probably gained access through the use of standard passwords. The system managers for all the open partition distributed processors were notified and asked to examine their logs for unauthorized activity. We learned from a review of earlier logs that the intruder had accessed machine G as early as June 23.

The intruder appeared to be interested in developing—developing a map of the distributed processors attached to the open partition of the network. Having gained access through an account with full system privileges, which had the password listed in the Digital Equipment Corp. manual, the intruder could access the open partition distributed processors, but could not reach the worker computers in the open partition proper. Activity logs led us to an account which had been created by the intruder, which we immediately destroyed. Later, we found indications that a program may have been executed and that the accounting records may have destroyed—may have been destroyed by the intruder.

Again, let me emphasize that no classified or sensitive data was available on these machines.

The security division reported the penetration of the open distributed processor network to the DOE area and operations offices and to the FBI on June 29.

The machine G system manager immediately changed all passwords to privileged accounts and the computing division was asked to modify Telenet access to force a sign-on by the network security controller. This change was made within 48 hours.

A meeting of distributed processor system managers was called on July 19. The system managers were instructed to make sure that their systems did not have any privileged accounts with identical user numbers and passwords, or passwords published in the Digital Equipment manuals. They were also instructed to review the privileged accounts and verify that users with privileges actually had a need for such access.

The director of the laboratory issued a memo laboratory management emphasizing the importance of security in our open computers. This established the requirement that written approval from the laboratory computer protection program manager must be obtained prior to any major changes to the open partition or its distributed processors.

Further controls were initiated by the computing division, with the cooperation of Telenet, to assure that a Telenet user is authorized to access the Telenet link to Los Alamos.

This incident happened because we connected Telenet, a known target for hackers, to an open computer and did not take full advantage of the available deterrents. These deterrents have now been implemented and we have seen no further successful intrusions.

The financial losses to the laboratory were not large. The Telenet and computer time cost less than $300. This disruption, however, required 3 to 4 work months of effort on the part of systems managers and security personnel in establishing exactly what the intruders had done.

And what could they have done? I cannot go into detail in an open forum, but the intruders could have caused confusion, delay, and perhaps incorrect results for many users of the open distributed processors.

I would like to close by pointing out that we must be realistic about access to open computing systems. The Los Alamos National Laboratory is a national resource and, as such, does a great deal of unclassified, nonsensitive computing in collaboration with the rest of the academic and scientific community. This work is important and can only be accomplished by providing mutual access to appropriate computing resources for researchers around the country. The security built into our integrated computing network allows us to do this without jeopardizing classified or sensitive information, but unauthorized accesses of the kind we are discussing today will occasionally occur in open computers. And must, and will, do what we can to minimize unauthorized access, but we must also realistically balance the benefits of shared computing against the risk from such events.

There are areas where the entire computer security community needs help. First, there are not enough people with the proper expertise and training in computer security. Programs to develop such individuals are badly needed.

Second, better low-cost methods for identifying computer users are needed. The password systems in use today are vunerable to attacks based on lost or stolen passwords and do not provide us with sufficient confidence that the user can be accurately identified. On the other hand, systems that can provide greater confidence are too costly for most applications.

Third, a much wider use of encryption would make a major improvement in the security of computing systems. The development of inexpensive encryption devices would lead to systems which are much more secure than those currently in use.

Finally, we need a realistic attitude toward those who abuse information processing systems. Obtaining unauthorized access to a government or private sector computer is not a game. At best, it is a willful act little different from a joyride in a stolen car. Given the equipment, knowledge, and preparation necessary to accomplish even the unsophisticated intrusion being discussed today, it is more realistically compared to breaking and entering a Government office. We should not dismiss the culprit because the office had windows.

Mr. Chairman, members of the committee, I thank you for this opportunity. And that's the end of my prepared statement.

Mr. **Glickman**. Thank you, Mr. McClary. We appreciate your coming here and the sensitivity of discussing some of these problems, and I, again, would like to commend you for coming here.

I want to go back to how you discovered the break-in, or the unauthorized access to your system. On page 4 of your testimony, you indicated, "Late on June 28, 1983, the system manager for machine G discoverd unauthorized activity under a privileged account."

Had this been going on for a while? What tripped the machine operator to know that there was unauthorized activity?

Mr. **McClary**. The—this is not the machine operator; this is the system manager for that machine.

Mr. **Glickman**. OK. The human being.

Mr. **McClary**. Yes.

In the open partition in particular, the systems managers and the other people who are responsible for the machines have been perhaps our strongest ally in detecting misuse of the computers. They're—he was watching the machine, he was on the machine, and he saw someone using it who he thought was unauthorized, and he triggered the system.

Mr. **Glickman**. Do you know how long this had been going on before he triggered the system?

Mr. **McClary**. No. When we went back and looked at the logs, the earliest we saw, I think, was June 23. I believe that's what's in the statement.

Mr. **Glickman**. I'm sorry. What date did you say?

Mr. **McClary**. June 23, I believe.

Mr. **Glickman**. And, so, it had just been 56 days then.

Mr. **McClary**. That's as far as we know.

Mr. **Glickman**. That's as far as——

Mr. **McClary**. You could never say for sure that they weren't there earlier, but that's the earliest date we have them detected.

Mr. GLICKMAN. And again you said that the only conceivable point of access was in the open system. That is, nothing else was jeopardized or could have been jeopardized?

Mr. MCCLARY. No. They couldn't have gone from the distributed processors, which are attached to the open partition through a gateway computer. They could not have gone with the knowledge they had from the distributed processors, even into the open partition of the network proper. There's a gateway computer between them. They have to know our ICN password and identification numbers to get from a distributed processor to the open partition proper at the ICN.

Mr. GLICKMAN. And that's what you mean by the words "with the knowledge they had," then? They would have needed that additional information to get in?

Mr. MCCLARY. Yes, they would have had to somehow gotten hold of a Los Alamos password.

Mr. GLICKMAN. And to get a hold of those passwords would have been obtainable only through some illegal leaking of that information from an existing employee?

Mr. MCCLARY. Carelessness, yes.

Mr. GLICKMAN. Or carlessness?

Mr. MCCLARY. Surely.

Mr. GLICKMAN. Where do you keep your passwords? Where do you keep all that information?

Mr. MCCLARY. The passwords are generated by our computer security group and given to individuals. The passwords for the secure partition are classified in themselves. They're classified at the level of the information they allow access to. That would be secret or confidential.

The passwords to the administrative partition of the network are administratively controlled. They're OUO information.

The passwords to the open partition are the responsibility of the individual user.

Mr. GLICKMAN. Is it technically possible to have gone from the open partition into some of the secure or non-open partitions?

Mr. MCCLARY. Technically impossible is a strong word. Yes, it is impossible to go——

Mr. GLICKMAN. Now wait. Is it technically possible to go?

Mr. MCCLARY. No. The—you always worrying about saying completely not possible, but our ICN is protected by making sure that each element that controls the partitioning of the network is a dedicated computer with no access by users—that is, users cannot execute any code on the elements of the network that separate the partition.

Mr. GLICKMAN. So you're saying that it is then impossible to——

Mr. MCCLARY. Yes.

Mr. GLICKMAN [continuing]. To have gone from one system—the open system to the close system?

Mr. MCCLARY. Definitely, yes.

Mr. GLICKMAN. However, if you were privy to a variety of information, you could have worked through the inside, right, if you would have known some of the passwords or obtained some of the intelligence?

Mr. McCLARY. You know the passwords to the different partitions and you have an authorized account and you have your management's authorization, yes.

But not from the open partition.

Mr. GLICKMAN. But not from the open partition.

Mr. McCLARY. Right.

Mr. GLICKMAN. Have you noted other attempts to break into your system before?

Mr. McCLARY. We have seen internal misuse of the computers and one other incident that I'm aware of of external access through Telenet.

Mr. GLICKMAN. When you say internal misuse of the system, could you describe that?

Mr. McCLARY. Yes, people misusing the systems for their own benefit rather than for laboratory benefit.

Mr. GLICKMAN. Is that a frequent happening?

Mr. McCLARY. No. Very infrequent.

Mr. GLICKMAN. How would they use it for their own benefit? In what regard?

Mr. McCLARY. Doing their tennis ladders, inventories of collections, and so forth.

Mr. GLICKMAN. Doing their what? I'm sorry.

Mr. McCLARY. Tennis ladders, inventories of collections, this sort of thing, keeping personal data.

Mr. GLICKMAN. OK.

Has their been access, external access, since this thing has occurred?

Mr. McCLARY. No. We have seen attempts. They have not been successful. Those attempts have been reported to the FBI.

Mr. GLICKMAN. And the 414's gained access to your system through the network through Telenet. Are you also connected to other networks?

Mr. McCLARY. Yes; we are.

Mr. GLICKMAN. How many?

Mr. McCLARY. Five, I believe.

Mr. GLICKMAN. And they perform the same function as the Telenet system?

Mr. McCLARY. No. There's a fundamental difference between the other networks and Telenet. The other networks are rather small, if you like, professional networks. Telenet is a large national communications network. It's a big target for hackers. The others are not.

Mr. GLICKMAN. Thank you.

Mr. Carney.

Mr. CARNEY. Thank you.

You made a very strong final statement there about what you think should be done, "it's more realistically compared to breaking and entering a Government office."

Let me ask you this question, Mr. McClary. Do you have a football pool on your computer?

Mr. McCLARY. No.

Mr. CARNEY. Are you sure about that?

Mr. McCLARY. No.

Mr. CARNEY. Did you ever have one?

Mr. McClary. I'm not sure.

Mr. Carney. You're not sure about it?

Mr. McClary. Right. I don't.

Mr. Carney. I suspect that every Government computer in operation that's not one that's secured probably has the results of last week's football game on it right now.

Mr. McClary. I wouldn't be surprised.

Mr. Carney. Would you suggest that that is the same as breaking and entering?

Mr. McClary. I beg your pardon? Now you asked me if I had a football pool.

Mr. Carney. I'm saying I would suggest that out at Los Alamos, the football pool is probably on the computer.

Mr. McClary. Yes.

Mr. Carney. Would you agree?

Mr. McClary. Yes.

Mr. Carney. Would you agree that's breaking and entering?

Mr. McClary. No. That's equivalent to using the supplies that I provide, that the laboratory provides for keeping. That's equivalent to using a pencil and paper and other such things for my own use.

Mr. Carney. Let me ask you—I would respectfully disagree with you on that. You know, the Government isn't buying the computers to run the football pool on, and you're getting the same access as that young man did.

Mr. McClary. No. I have a—what you're talking about is misuse by an authorized user. The person who put the football pool on is an authorized user of our network. He's misusing it. He's misusing his authorization.

Mr. Carney. Let me——

Mr. McClary. What I'm talking about when I make the comparison with breaking and entering is someone who is not authorized access coming into a Government computer system. I think there's a fundamental difference between those two approaches.

Mr. Carney. I think the fundamental difference is they didn't steal anything and the pool does.

But, anyhow, that's neither here nor there.

Let me ask you about the password.

Mr. McClary. Yes.

Mr. Carney. Was it a common password that you had for your computer?

Mr. McClary. Yes. It was one of the passwords that Mr. Patrick described that is published in the manual, the deck manual.

Mr. Carney. Would you agree that the password—changing of the password—would be sufficient enough to, say, eliminate 95 percent of this type of access?

Mr. McClary. Yes.

Mr. Carney. Would you have any suggestion—we asked the previous witness if they had any suggestion to what type of action the Federal Government could take. Would you have any suggestion as to what course of action we should take from a legislative standpoint?

Mr. McClary. I think the main thing that needs to be done is we need legislation to provide the kind of protection for our informational resources that we provide for our physical resources. I think we're moving from a society where most of the value is associated with property to one where information is becoming more valuable. I think what we need is legislation that will provide the appropriate protection for those information resources. And I think that's where the distinction between what an authorized user and what an unauthorized does and those analogies with physical security come into being.

I don't have any specific recommendations for how to write a law. I'm not a lawyer. But I do a——

Mr. CARNEY. How about unintentional—I'm sorry.

Mr. McCLARY. But I do have a recommendation for the goal. And the goal of your efforts should be to provide the same protection for information resources that we provide for our materials resources.

Mr. CARNEY. How about unintentional intrusion? How would you handle that?

Mr. McCLARY. Unintentional trespass occurs, and our legal system handles it quite well, I think. I would, again, draw the analogy with the protection of material assets and draw laws that are very analogous. Intent enters into much of our legal system, and I think it can handle it.

Mr. CARNEY. Isn't it quite true that you could be trying to access a computer which you have the right to access and unintentionally access your computer?

Mr. McCLARY. I think that would be extremely difficult to do. Very unlikely. I know—

Mr. CARNEY. Would you have thought a year ago it would be extremely difficult for a group of young men in Milwaukee to access your computer?

Mr. McCLARY. The open computers?

Mr. CARNEY. Right.

Mr. McCLARY. I wouldn't—we were not shocked when this occurred. We were disappointed that some of the system managers had not changed their passwords. But the nature of open computing is such that things like this are going to occur occasionally. Just like in physical security or protection of assets, if you set up a system to protect from the theft of tools in an open public area—say, one at the laboratory—and you also have a system that protects against the theft of special nuclear materials, you're very surprised if anything happens to the more valuable assets, classified information, special nuclear materials.

But, occasionally, a theft occurs of materials from an open area, one protected perhaps by a lock and a key, because someone lost the key and it's picked up by someone who'll use it to gain access and take tools. It's going to happen occasionally.

We were not shocked, just as we were not shocked when some tools were stolen from an open laboratory——

Mr. CARNEY. But you were shocked that some of your managers did not change the passwords?

Mr. McCLARY. We were disappointed.

Mr. CARNEY. Not shocked?

Mr. McCLARY. Disappointed is better, I think.

Mr. CARNEY. You were disappointed——

Mr. McCLARY. Yes.

Mr. CARNEY [continuing]. That some of your managers did not.

So you could have had, by using such a common password, and if your access number was similar to someone else who was sharing Telenet, for instance, you could have had unintentional access by someone who had every right to be using Telenet to access a computer that he or she had the right to access; is that not correct?

Mr. McCLARY. I could conceivably sign on to Telenet and make a typing mistake and get onto the wrong computer. As soon as I accessed the computer, got onto the computer proper, and realized that my programs or the programs that I wish to use are not there, I would get off, and I wouldn't come back.

Mr. CARNEY. How long—well, have you ever dialed the wrong number twice?

Mr. McCLARY. Yes.

Mr. CARNEY. Well, then, I'm not sure you wouldn't come back.

How long would it take you before you were cognizant of the fact that you didn't have the information on the computer that you accessed?

Mr. McCLARY. When you—after you sign on to the computer and when you've gone to execute whatever task you wanted and you found that your task or your data was not there, you should know you're on the wrong computer.

Mr. CARNEY. OK.

Mr. McCLARY. Assuming the identification that went from the computer didn't tell you.

Mr. CARNEY. OK.

Now we're moving up a step. We accessed the computer, and you assume you're on the computer you tried to access, now you have to feed that computer some additional information to get information out, to get the program you're looking for, correct?

Mr. McCLARY. You have to tell it what you're looking for, yes.

Mr. CARNEY. OK.

Were the 414 gang capable of telling that computer what it wanted to access, some information that you had put on that computer out of it?

Mr. McCLARY. I don't believe I understand the question.

The 414's knew a password in an account. So they got onto Telenet, came to a computer, used the standard passwords then to gain access to that computer, so now they are a user of the computer.

Mr. CARNEY. OK. Now they're on the computer.

Mr. McCLARY. Yes.

Mr. CARNEY. Do they have to have a wealth of knowledge to get anything off of that computer?

Mr. McCLARY. No; not from that point. They have to be knowledgeable computer users.

Mr. CARNEY. In other words, if I broke the code, I probably could get the payroll account of—something like that—of a business computer, or get some general, not unclassified information, or——

Mr. McCLARY. Well, at Los Alamos——

Mr. CARNEY [continuing]. Proprietary type——

Mr. McCLARY. Well, I can't speak for other places, but at Los Alamos, you cannot get any classified or sensitive unclassified information, such as the payroll or personnel.

Mr. CARNEY. But a common—not a common—but a person who has familiarity with a computer and its operation could probably very simply get, let's say, things like payroll and accounts receivable and that type of thing off of computers?

Mr. McCLARY. You mean other than Los Alamos?

Mr. CARNEY. It's a standard software package?

Mr. McCLARY. No. I——

Mr. CARNEY. See, where I——

Mr. McCLARY. Again, I can't speak for other places——

Mr. CARNEY. Right.

Mr. McCLARY [continuing]. Besides Los Alamos——

Mr. CARNEY. I appreciate that.

Mr. McCLARY [continuing]. And they protect their information.

Mr. CARNEY. But what I'm confused at—I can understand how to get the access, but not your computer is a storage facility for data.

Mr. McCLARY. Yes.

Mr. CARNEY. There has to be some way to stimulate that computer to spew out the data that you're looking for.

Mr. McCLARY. Yes. You have to get access to the data itself, or to the program that you're after.

Mr. CARNEY. OK. My question is does it take an enormous amount of talent to get to that step? Accessing it is one thing. It's like dialing the phone number. But to get that computer to give information back to you, specific information back to you——

Mr. McCLARY. It takes quite a bit of knowledge and ability probably to get specific information. However, if you just go poking about in a computer, then you take what you find. And that's generally the way the hackers do, I believe. They just look around and they find a program or an account and they execute it and see what it does.

Mr. CARNEY. Well, these accounts that you talk about and programs, are they commonplace? You know, for simplicity, does a payroll account usually access the same way in many computers?

Mr. McCLARY. No. I think it—if I understand your question, I think it depends on the programer responsible for the program. He—he has named it, set up protection for it——

Mr. CARNEY. For each account.

Mr. McCLARY [continuing]. Set it up. It depends on what he does. It's very variable over different computer systems.

Mr. CARNEY. I understand—we'll be specific, we talk about the intrusion that you had that we're talking about here today. And I understand that it's still under investigation. Maybe you cannot tell us.

But did they access any information off of your computer, or did they just get in and kind of look around?

Mr. McCLARY. As far as we can tell, they essentially got in and looked around. They came in, set up a—came in using the published password—set up an account, we believe, and then looked around through the system. They may have executed a program, but we can't make a definite conclusion on that, because some of the accounting records also disappeared. We don't know if they destroyed those or not.

Mr. CARNEY. I see.

Mr. McCLARY. So all we know that they did is come in, look around the open distributed processor, and set up that one account and just look about the system. We saw no damage, no residual damage from them.

Mr. Carney. Do you think that this is the only time you have been accessed?

Mr. McClary. No. I would doubt that.

Mr. Carney. In other words, you think perhaps you have been accessed by other hackers?

Mr. McClary. We can't say that we haven't, so I would not be surprised to find another incident of that.

Mr. Carney. And there's no way you really could tell; is that correct?

Mr. McClary. Not necessarily.

Mr. Carney. Well, thank you very much. I appreciate your answers.

Mr. Chairman, I yield back the balance of my time.

Mr. Glickman. Thank you.

Mr. Gore.

Mr. Gore. When they set up an account there, that wasn't the one where they used Joshua for the password, was it?

Mr. McClary. I believe they did use Joshua at Los Alamos.

Mr. Gore. That's an uncomfortable mixture between fact and fiction, when you have this movie and the nuclear control center is penetrated by computer hackers discovering the password "Joshua," and then a few months later—or a few weeks later—the computer system at Los Alamos is penetrated and they put the word "Joshua" as their password to access the Los Alamos computer from then on. That's absolutely incredible.

Mr. McClary. It's gets your attention.

But I must remind you again that Los Alamos does more computing than the nuclear weapons computing. That's all done in the classified system.

Mr. Gore. I'm going to come to that.

Mr. McClary. OK.

Mr. Gore. I understand.

Mr. McClary. They did not penetrate that.

Mr. Gore. Was yours the computer that they programed to answer Joshua by saying "Would you like to place a nice game of chess, Dr. Falcon?"

Mr. McClary. No; I don't believe so.

Mr. Gore. That was another one. OK.

I understand what you're saying about the partition between—you had one open operation, and then you had a lot of other computer operations that were partitioned away from the open terminal. That's the essence of what you were saying.

Mr. McClary. Yes. Essentially, we divided the computers into groups based on the sensitivity of the data that they processed.

Mr. Gore. Yeah. Well, now, if I understood Neal Patrick's testimony earlier, he said that, after getting into your open terminal there at Los Alamos, that gave them access to a whole lot of other computer operations that had plugged into your open terminal.

Mr. McClary. Yes. The open partition, the distributed processors attached to the open partition of our ICN, talk to other computers around the country.

Mr. GORE. Well—and then they could, through your computer port, they could then get into the other systems that talk to your terminal.

Mr. MCCLARY. Yes; that talk to the open—the distributed processors on the open partition.

Mr. GORE. Well, now, are you satisfied that all of the—all of the other systems that were talking to your computer through the open terminal were also un-unclassified data bases?

Mr. MCCLARY. The only ones that we allow onto the distributed processors attached to the open partition are unclassified systems.

Mr. GORE. Well, how do you control that?

Mr. MCCLARY. How do we determine that they're unclassified?

Mr. GORE. Let's suppose somebody at the National Security Agency, for example, wanted to communicate with Los Alamos and did so by contacting your open computer terminal. How do you know whether or not the National Security Agency is contacting you with—by using a computer that has an unclassified data base? How do you know that somebody is not in a hurry and just contacts your open computer port for the information they're looking for?

Mr. MCCLARY. The same way that you know that someone in Washington doesn't pick up a telephone and call someone at the laboratory and discuss classified information over that open telephone line.

Mr. GORE. Well, I don't know that.

Mr. MCCLARY. That's right.

We do not—we get certification from each person who connects to our open partition that they are doing only unclassified, unsensitive information. We inspect files on the INC at random to see if we detect information in the wrong partition.

Mr. GORE. Yeah, all right. Maybe—maybe the lack of understanding is on my part. But let me rephrase the question again.

You're getting certification from them that they're not using classified—that they're not putting classified data through your computer.

Mr. MCCLARY. We tell them that they are not allowed to, and we ask them to agree not to do that.

Mr. GORE. OK. Now, suppose they don't——

Mr. MCCLARY. We also provide, of course, secure access to the secure partition of the network. We provide ways for legitimate users to get secure information—classified information into our secure network.

Mr. GORE. OK. Here's the point. Here's what I'm trying to get at. You got your computer port here.

Mr. MCCLARY. Yes.

Mr. GORE. Somebody else at another government agency has its computer and it contacts yours, OK?

Mr. MCCLARY. Yes.

Mr. GORE. They may not be using classified data in the communication between their computer and yours, but they may have it on their data base. See what I'm saying?

Mr. MCCLARY. No; I—Dotty is the computer protection program manager for the laboratory, and the computer security officer for the laboratory.

Mr. GORE. All right. Let's say they—let's say they got five programs—five computer programs on their data base, just as a hypothetical. They're using one of those computer programs to communicate with your open terminal. All right. The information that's being exchanged and dealt with through that one computer program is unclassified. One of the other four may have some classified data because they're using their computer to talk with yours.

OK, here comes the 414 Club and they access your terminal and, through that terminal, they gain access to the—to the other computer that's communicating with it. Then if they gain access to—not just to the program that's—that's the subject of the dialog between the two computers, but the others that are not at that point in use between them, is that something that's—that's—that's possible?

Mr. MCCLARY. Excuse me. I think I see what you're aiming at now.

Mr. GORE. Yeah.

Mr. MCCLARY. The DO—the DOE regulations and requirements do not allow anyone to have both connections between a—connections to open and secure systems. There's—you have to have a—an approved system to process classified information before you process classified information. That will not be approved if there are any connections of the nature that you're describing to an open computer system.

Mr. GORE. Uh-huh.

Mr. MCCLARY. So those connections are not——

Mr. GORE. They're not supposed to exist.

Mr. MCCLARY. That's right. They are not supposed to exist.

Mr. GORE. Uh-huh. Well, hopefully, the computer security folks will—will look into ways to make certain that doesn't happen.

Now, are you familiar with the speculation about radio waves giving radio frequency interference being used to reconstruct the activity on——

Mr. MCCLARY. Do you mean emanations—compromising——

Mr. GORE. Correct.

Mr. MCCLARY [continuing]. Emanations from equipment?

Mr. GORE. In other words, no telephone lines involved. You've got a computer at Los Alamos and somebody has a car in the parking lot with a receiver that's capable of picking up the radio interference and, from those radio waves, reconstructing the movements of the central processing unit and—and—and printing out what it is that's occurring on your computer?

Mr. MCCLARY. Yes; this is the so-called tempest problem. And——

Mr. GORE. Tempest problem?

Mr. MCCLARY. Yes.

Mr. GORE. As in tempest in a teapot?

Mr. MCCLARY. No; it is not——

Mr. GORE. OK.

Mr. MCCLARY [continuing]. A tempest in a teapot.

Yes; we are familiar with that problem. We have a special section within Dotty's group at Los Alamos who work on the tempest problem, or the problem of compromising emanations from our computing equipment.

We've established policies in the last few years that require the use to tempest-approved equipment.

Mr. GORE. Yes.

Mr. MCCLARY. That is, equipment that has been tested to eliminate that problem on all classified systems.

Mr. GORE. So—so you are well aware of that and working with it and——

Mr. MCCLARY. Yes; I think we have——

Mr. GORE. I'm told that, for example, an electric typewriter, with the proper equipment, one can listen to the waves emanating from an electric typewriter and reconstruct everything that the typewriter is typing.

Mr. MCCLARY. I can't comment on that, except to say that we're aware of the tempest problem and we do require the use of tempest-approved word processors and computers for classified information.

Mr. GORE. All right. One final question. You talked about disruption. You said there was some disruption within your computer by those who—who gained access?

Mr. MCCLARY. I did not mean to say that they disrupted the computer system. They came in and they created an account. They may have executed a program. The disruption came mainly for the people involved with the systems and for security personnel in determining what had happened.

Mr. GORE. I see.

Mr. MCCLARY. And why it had happened.

Mr. GORE. But when they gained access, they were actually able to program your computer themselves to an extent; is that correct?

Mr. MCCLARY. Yes; the way they gained access gave them the privileges of writing programs and executing programs.

Mr. GORE. Are you familiar with the classic cookie monster program that was reported at MIT?

Ms. CAMILLO. Not familiar with it, but we've heard about it.

Mr. GORE. I'm told—I'm reading from a Newsweek article about this where one of the hackers at MIT programed the main computer there to—to run the cookie monster program. And the way it worked was when someone working on the computer least expected it, the screen would suddenly flash the word "cookie." If the programer didn't immediately respond, then the cookie monster would go berserk writing "cookie" over and over and over again, obliterating whatever was on the screen, and ending up by demanding "Give me cookie." The only way to stop the monster was to feed it by typing in the word "cookie."

But you didn't have that kind of disruption at Los Alamos?

Mr. MCCLARY. No.

Mr. GORE. You just had Joshua.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Just briefly, before we go on, and following up on Mr. Gore's question about these folks could program—could program in something, could there be a logic bomb in the system now? Could they have programed something in that——

Mr. MCCLARY. That we did not find?

Mr. GLICKMAN. You may have not found it yet.

Mr. MCCLARY. That's right.

Mr. Glickman. But could there be something in that system now that they programed in that could come back to haunt Los Alamos at some point later on?

Mr. McClary. It's conceivable that there could be; yes.

Mr. Glickman. Is there any way to find that?

Mr. McClary. I know of no way to guarantee that there's not one.

Mr. Glickman. You know, that seems absolutely incredible to me that the systems are incapable of determining if somebody has intentionally sabotaged or jeopardized them. That is very, very worrisome that you can't cleanse the computer to determine what's in there.

Mr. McClary. Two of the biggest problems in computer security right now are software and hardware verification. That is, software verification is the question of, is the program that I'm running really the one that I wrote and expected to execute? That's an extremely difficult problem, one that's well worth solving if we can. That's the problem you're talking about, the problem of determining that the program you are running is the one that you think you're running, that no one has added something to it or changes something. It's not a simple problem.

Nor is hardware verification, verifying—which can't be done remotely, of course—but verifying that someone hasn't come in and modified your hardware.

Mr. Glickman. Yeah. I'm just amazed at the fact that—not these—necessarily these young folks—but anybody could have programed something to take effect a year from now or 2 years from now, or when something else happens with respect to the operations of the system that totally could disrupt the operations of, let's say, the open system. Or let's say there's a change in the next year and you change your methodology between talking between your computers or systems that could violate something later which could not be violated right now, and you don't know about it and can't find out about it.

Mr. McClary. Yes. As I say, software verification is a very difficult problem. No one really knows how to do it right now.

Mr. Glickman. Mr. Nelson.

Mr. Nelson. Thank you, Mr. Chairman.

And thank you, Mr. McClary, for giving us a better concept of the way that you compartmentalize at Los Alamos in order to provide the security you need.

I want you to amplify, please. Earlier you stated something to the effect, we need the same protection for information resources as we provide for our material resources.

Mr. McClary. Yes. I think that—I think there's a fundamental change here or coming in our society, and that's the increasing value of our information resources. We worry about exporting technological information, we worry about protecting all sorts of information. For a long time we worried about protecting physical goods, material goods. And I think we're going to have to come up with legislation and techniques that provide the same protection to our information resources and our information capabilities as we give to our material capabilities. I think that should be the goal of our legislation.

Mr. Nelson. You think that, from your experience, that that is not provided?

Mr. McClary. No. I think what's happening is the technology of computing and the cost of computing power, the technology is going—is improving so rapidly, the cost of computing capability is dropping so rapidly. I paid $39.95 for a computer in a drug store the other day that is really quite a capable computer. I took it home just to have a $39.95 computer.

But what's happening is, as the technology increases and the cost per unit of computing capability drops, our computer security capability is not keeping up with it. We need more people who are computer security capable. As someone said a while ago, we definitely need more education of the users on the importance of computing.

Part of the problem for systems managers is that the systems change so rapidly, both in hardware and software, and the pressures on them are to deliver computing results, of course, they need education as do others on the computer security aspects that must go along with the changing technology.

Mr. Nelson. Now, are you specifically suggesting computer security by virtue of—you say hiring more people in——

Mr. McClary. Training more people and educating more people.

Mr. Nelson. And in so doing, so that they write software that is additional security measures for——

Mr. McClary. So that they——

Mr. Nelson [continuing]. Existing computer systems?

Mr. McClary. Yes. Or they develop ways to verify software or verify hardware or develop low-cost encryption devices that will allow us to transmit information across telephone lines in encrypted form, so that even if it's intercepted, it won't mean that much.

Mr. Nelson. OK. At the end of your statement, you put it rather bluntly and rather strongly that unauthorized access is—and I'm quoting you—"more realistically compared to breaking and entering a government office.

Mr. McClary. Yes. I——

Mr. Nelson. Could you give us your conclusions why you feel as strongly as you do?

Mr. McClary. Yes. Because I don't agree that what the 414's and similar groups have done is simple and easy. What they did—they had to go out and they had to get very sophisticated gear. They had to learn—they had to add telecommunications gear to their computing gear. They had to learn how to get into Telenet and similar networks.

Then they had to read deck manuals and study deck manuals. I don't think—I don't know how many of them owned or used digital equipment computers and had deck manuals available. But they had to go out and learn how to do this. It's not a simple thing to do. And then they had to do it over and over again.

To me, that's more preparation than it takes to walk up to an open public area and break out a window, for instance, and go in. It takes more work to do that.

Mr. Nelson. All right. With that as background, in another one of your statements in your testimony, you said that the actual computer time cost was less than $300.

Mr. McClary. That's Telenet and computer; yes.

Mr. NELSON. All right.

You further said, however, there was 3 to 4 work-months of effort on the part of your managers and security people in establishing exactly what the intruders had done.

Mr. McCLARY. Yes.

Mr. NELSON. Do you think that, as a deterrent, then, to this kind of activity, that—that the Government ought to be compensated for that cost that was incurred as a result of this break-in?

Mr. McCLARY. I think that we should have laws that give people—that make people account for the damage and the cost that they cause others to incur, just like we do in material property protection. You should be reimbursed for damages.

Mr. NELSON. Earlier, lest there might have been any misunderstatement in a comment that I made to Mr. Patrick in which I said that I was thankful for calling attention to the problem, I want to make sure that the committee members here understand that I was—I am thankful for the focusing of the national attention on what I believe to be a problem that has been with us for some time, but that the Nation's attention was not riveted to the fact. I want to make sure that folks do not imply by that gratefulness any statement on my part of being thankful of the actual activity which caused this unauthorized access to occur on yours or any other computers. But sometimes it takes this kind of activity to rivet the attention, as this obviously has done here in the Nation.

You have been a most articulate witness, and I appreciate your statements, and I appreciate your strong statements.

Mr. McCLARY. Thank you.

Mr. NELSON. Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you.

Mr. Wyden.

Mr. WYDEN. Thank you, Mr. Chairman.

I, too, think you've been an excellent witness, Mr. McClary.

I just have one area I want to explore with you. One of the things that I have sensed, and we saw it in the small business hearings we had, and it is really one of the concerns behind my legislation, is that all across this country, we're seeing people spending enormous sums of money for computer systems, enormous sums of money for software systems, for hardware systems, for this incredible constellation of computer equipment. And it strikes me we spend very little for security.

And I was wondering if you could break down for us the amount of dollars you spend on your system, your hardware and your software, in correlation to what you spend on security, because I think that would be helpful and—I know you don't walk around with these figures right——

Mr. McCLARY. You're correct.

Mr. WYDEN [continuing]. Off the top of your—give us a ballpark. Give us a ballpark.

Mr. McCLARY. I'm sorry. There are like—there are over 600 computers at Los Alamos.

Mr. WYDEN. Even a ratio. You think you spend 2 percent on security?

Mr. McCLARY. On computer security?

Mr. WYDEN. Yeah.

Mr. McClary. I'm sorry. The magnitude—to make that estimate right now off the top of my head, I can say that Dotty's—let me—we have 17 people in the computer and telecommunications security group at the laboratory, compared to a total laboratory population of perhaps 7,000 employees using about 600 computers. I don't have the monetary figures with me to give you the comparison of the cost, the moneys spent on communications security, because you would have to go back through the system, look at the cost of using dedicated computers to separate the partitions. I'm sorry. I just don't have that with me.

Mr. Wyden. I would like you to furnish to me as an individual Member of Congress. If the chairman was so inclined, perhaps he'd want to request it for the committee as well. I realize it's a lot of work, and I ask with a very specific point in mind——

Mr. McClary. I understand.

Mr. Wyden [continuing]. That I sense all over this country, in the private sector and in Government, we are embarking on a tremendous expenditure of funds for software and hardware systems, and very little is to be spent on security. And one of the things that I have considered is whether or not the Congress should require that this be a budget item, that agencies that receive funds for computer systems, hardware and software, should require as a budget item that a certain amount be spent on security.

Would you support that as a general kind of proposition?

Mr. McClary. I think, as a DOE contractor, I'm hesitant to answer that question. I think there should be an appropriate amount of money spent on computer security.

Mr. Wyden. How are we going to get it done if we don't require it as a specific budget item?

Mr. McClary. I support providing the funds for computer security. No question about that.

The mechanism, I think, has to be worked out, not by the security types, but by you and others involved in the legislative process.

Mr. Wyden. The only other question I had, very briefly, I wanted to come back——

Mr. McClary. Before we leave——

Mr. Wyden. Yeah.

Mr. McClary [continuing]. Would you state exactly what you want me to supply?

Mr. Wyden. Yeah. What I would like is the dollars, aggregate dollars, that you spent for your software and hardware systems.

Mr. McClary. For our computing systems?

Mr. Wyden. That's correct.

And then I'd like to see the dollars that you spend on security, because I'm very concerned about that ratio. I saw it when we had our hearings on the problems of small business, is that every small business, you know, once a system feels they got to have it but is concerned about the expenditures on—on security and then doesn't wake up until it's too late.

And the reason I want to have this information is that one of the things I may ask my colleagues to push for is that there be a specific budget item built in every Government security system that says it be spent on security and security kinds of—kinds of features.

So I'm not asking this idly. I'd like it as one Member of Congress. If the Chair wishes—wishes it as well, I can give it to him or they can request. But I do it with a very specific purpose, and that is that I think that may be one—one legislative area that Congress needs to get into.

One other question very briefly, and that is do you know of any management or technical initiatives that you all are pursuing to control the misuse by the authorized users? I'm thinking particularly about this football kind of—the football pool kind of analogy. And I—I want to make it very clear I'm pro football, and I'm not coming out here today against football. But it's awfully hard to draw the line, because misuse of service, presumably, is misuse of services, and the Government suffers, you know, a loss. And I'm curious whether you all are pursuing any initiatives to control misuse by the authorized users, whether it is football pools or——

Mr. McClary. Yes. We have a program mandated under DOE order 1360.2 which implemented A-71 to prevent misuse of Government computer systems.

Dotty is the—

Mr. Wyden. I'm glad you explained that and didn't just leave us with the numbers.

Mr. McClary. Yeah. It's a program intended to prevent misuse of Government computing systems. Dotty is the Computer Protection Program Manager. That is the person in charge of that program at Los Alamos. And that's the program that uncovered the situations we discussed earlier.

Mr. Wyden. Those—those DOE rules have penalties for violations, or what do they consist of?

Mr. McClary. No. The penalties, they have requirements that we prevent the misuse, that we set up a system which will detect and prevent misuse. The punishments then—or the penalties, if you like—are the responsibility of the organization, in this case Los Alamos.

Mr. Wyden. Thank you very much.

Thank you, Mr. Chairman.

Mr. Glickman. Let me just ask you, rather than necessarily providing more money, where in the organizational structure in Los Alamos is the security organization, and how high do you report?

Mr. McClary. We report to the Associate Director for Technical Support, and he reports directly to Don Kerr, the Director of the Laboratory.

Mr. Glickman. So you think that in terms of at least the structure, you are given a place high enough to have some input?

Mr. McClary. Yes. We're—we're very happy with the support the laboratory has given security at Los Alamos National Laboratory. Some years ago, they took all the elements of security, including computer security and telecommunications security, and put them together into one organization under the Associate Director for Technical Support, and that's worked very well. We're very pleased with the management support security gets at the Laboratory.

Mr. Glickman. My final question is do you use tiger teams to enhance your security?

Mr. McClary. I don't think in this forum I can discuss that.

Mr. GLICKMAN. OK.

We thank you very much for coming here. We're most appreciative.

Mr. McCLARY. Thank you.

Mr. GLICKMAN. Our next witness is Donn B. Parker, senior management systems consultant at SRI; and he is accompanied by Geoffrey Goodfellow, also of SRI. I am informed Mr. Goodfellow has had some personal experience in some of these things before as well.

Mr. Parker, we're pleased to have you here. You are renowned as one of the world experts in computer security. I did read the article about you in People magazine within the last few weeks, and we are appreciative of your input.

Do you have a prepared statement?

Mr. PARKER. Yes.

Mr. GLICKMAN. OK.

Mr. PARKER. I wish to submit my prepared statement as read, and also Geoffrey Goodfellow wishes to submit his as read.

Mr. GLICKMAN. That's fine. Your entire statements will appear in the record.

You may feel free to proceed in any manner you wish. If you wish to summarize or outline, that's fine with us.

Mr. PARKER. Fine.

I'd like to start by having Jeff briefly comment from his prepared statement. Jeff.

Mr. GLICKMAN. OK.

STATEMENTS OF DONN B. PARKER, SENIOR MANAGEMENT SYSTEMS CONSULTANT, INFORMATIONS SYSTEMS MANAGEMENT DEPARTMENT, SRI INTERNATIONAL, MENLO PARK, CALIF.; AND GEOFFREY S. GOODFELLOW, SENIOR SYSTEMS ANALYST, SRI INTERNATIONAL, MENLO PARK, CALIF.

Mr. GOODFELLOW. Thank you, Mr. Chairman.

My name is Jeff Goodfellow. I'm—have been primarily employed by the computer science laboratory at SRI International in Menlo Park, Calif. for the last 10 years. And while at SRI, I've been involved in research efforts relating to packet switched computer network communications systems, protocols, and security technologies. I have also been involved in various operating and subsystem development projects.

Currently, my responsibilities include a position as principal investigator of SRI's involvement in a Department of Defense program aimed at developing and proving secure computer systems that operate at different security levels and communicate via networks.

A detailed biography of my career, from the seventh grade of school where I discovered computers, which eventually led to my permanent abandonment of the formal educational system during high school to how I got today—to where I am today with no degrees of any type of equivalency to my name, is included at the end of my testimony.

I am the coauthor of the "Hacker's Dictionary—A Guide to the World of Computer Wizards," a new book being published this fall.

The statements included herein are my own and do not necessarily represent those of SRI International or any of its clients.

What I would hope to do here today is to try and put the hacking problem in perspective for you, hopefully outline a little bit what—what can and should be done to help abate the hacker problem, and then comment on—let us not lull ourselves into a false sense of security that we might think that we would be in.

I guess I'd like to start out with by—by primarily letting everyone know exactly what—what the computer hacker can be defined as. And you can primarily define the computer hacker as—as one who enjoys learning or knowing the details of computer systems and how to stretch their capabilities, as opposed to most users of computers who prefer to learn only the minimal amount necessary to get their job done.

A computer hacker can also be defined as one who programs computers enthusiastically for the sheer fun of it, and gets a nonprofessional amount of enjoyment out of using them.

A computer hacker also is capable of appreciating the irony and beauty—in other words, the hack value—of a computer program.

And you can also say that a computer hacker is someone programs quickly or is an expert on particular program.

This definition and the proceeding ones are correlated, and people who fit them congregate either in person or via electronic media, such as bulletin boards and computer networks.

But unfortunately, hacking has a rather unsavory faction to it, a malicious or inquisitive meddler, or poacher, who tries to discover information by poking around. For example, a password hacker is one who tries, possibly by deceptive or illegal means, to discover other people's passwords. A network hacker is one who tries to learn about computer networks, possibly because he wants to interfere. One can tell only by the context, the tone of voice, and the manner of their approach.

Hackers of all factions, whether benign or of the unsavory flavor, consider themselves somewhat of an elite, though one to which new members are gladly welcome. Hacking is meritocracy based on ability. There is certain self—certain self-satisfaction in identifying yourself as a hacker. But if you claim to be one and you are not, the hacker community will normally excise you and will label you as bogus.

The hacker is intensely interested in technology and is a very inquisitive person. Many are social outcasts who don't enjoy the same things as most kids their own age. Hackers of the unsavory flavor are a very curious breed of individual. Many can be best described as loners looking for someone to appreciate their talents. They know full well what they are doing errs on the dark side of the force, to coin a phrase. Unsavory hackers want to get caught so they can be given the appreciation they deserve, and the process of getting caught adds an essence of thrill to their endeavor.

I would like to state for the record that benign hackers, such as I, deplore the unsanctioned entry and the subsequent rummaging of mainframe computer systems and networks. These types of activities are tarnishing the profession of hacking and giving it a bad name.

In the real world, computer systems—computer system organizations are generally run by totalitarian policy states. This unfortunate reality fosters resentment in hackers and a desire to challenge the reverence of authority develops. As a result, the way hackers bring themselves to a system manager's attention is via the medium they know and relate to best, a terminal and modem and your computer system. In most cases, the hacker wouldn't personally think or know of how to go about calling up the director of a computer system and offering his services to you as a bright young guy for the fear of reprisals or not being taken seriously. Instead, they choose to introduce you to them by meddling with your computer systems, cavalierly circumventing security and protection mechanisms, in order to satiate their hunger for knowledge and develop an understanding of how things work.

The organization will respond in kind by trying to plug the leak of an intrusion into their system by erecting barriers. This type of reaction is precisely the wrong approach to take, because the hacker will notice the beefed-up defenses and see them as a further challenge of his prowess and ingenuity and legitimate users are subjected to greater inconvenience.

Instead, what an organization should try to do is try to befriend hackers which have penetrated their inner sanctums. The perspective that should be taken is one of, is it helpful or useful for you do to this, rather than, are you authorized to do this? You must, in effect, come down to the hackers' level and circulate among them. Show them that you appreciate their talents. If you ask them nonforeboding questions and take a genuine interest in what they are doing, most of the time you'll find they're more than happy to tell you exactly what it is they're looking for or interested in. The hacker wants to learn, and you can be their guide or teacher.

This is how I was dealt with by the firm that caught me during my unsavory hacking dates in 1973, when I breached security on a large commercial time-sharing network and many of its host computer systems. I was very much inspired by this method of catching and steering unsavory hackers toward a more constructive use of their talents.

There is, however, a more virulent strain of the unsavory faction, namely, the electronic vandals or joyriders. Note well that these are not hackers. This strain includes, for example, kids whose parents are of an affluent nature. As a result, these kids have an inflated world picture and little or no true sense of reality due to the nature of their carefree lifestyles and upbringing. These kids plague computer networks and systems as they would spray-paint on school walls, tee-pee someone's house or engage in the use of so-called recreational drugs.

In other words, these illicit activities are engaged in with absolute reckless abandon and disregard for the rights or sovereignty of other people's property.

As with regular vandalism, the primary motivators seem to simply be doing it because they can get away with it and because of the respect it brings them among their equally disrespectful peers. This differs from the unsavory hacker in that there is no constructive purpose or motive involved, such as learning or acquiring knowledge.

This problem is further exacerbated by the juvenile age of the perpetrators and the unlikelihood of prosecution, even if caught. The perpetrators are smugly aware of their immunity in most cases.

What can and should be done to help abate the unsavory hacking problem?

From my own observations and inspections of systems, and from what I've been reading in the press, I have come to the conclusion that computer site administrators are not taking reasonable and prudent measures to protect their computer systems, even from the most casual methods of circumvention.

A rather egregious example of this would be the—would be of which—the installation of which the 414's allegedly logged into with user name "test" and password "test." User names and passwords of this sort are not uncommon, and sites which set up log-ins like this are simply asking for a break-in, just as someone who would leave the key in the lock on the front door of their house, complete with the welcome mat out for all to see, invites the casual burglar.

The way I view reasonable and prudent measures of protection from the casual penetration is by drawing a paradigm with the way the Department of Defense handles classified information.

With respect to the handling and use of classified information, it is the responsibility of organizations to which you belong, in conformance with Department of Defense guidelines, to provide you with rules and regulations in the handling of classified information. It is also the responsibility of your organization to provide you with a safe place, that is, vault to store said information and to provide adequate safeguards, such as alarm systems, security personnel, and patrols, to prevent unauthorized access.

The same methodology should be taken to heart by the administrators of computer systems. It's their responsibility to provide reasonable and prudent measures to prevent unauthorized access attempt from gaining access to the system. This means a few very basic things like forcing users to choose reasonable passwords, not their spouse's name or their dog's name; setting up proper modem control on dial-up and remote access ports so that disconnection causes any jobs or trojan horses left on that port to be flushed and results in resetting the port to not-logged-in status; reporting incorrect password attempts to the system console or log file; causing line disconnection after very few successively repeated incorrect password attempts; and using encrypted passwords so it is not possible to compromise an entire system's password list when circumvention of a system's protection mechanisms is attained. This is analogous to the DOD's compartmentalization of information, so a breach in one area does not sacrifice security in all areas.

The second facet of my paradigm is the user's responsibility. I don't go out to lunch and leave my secrets sitting on my desk. I put them in a vault. I don't go throwing them over embassy walls. So it is the same for the computer system user. It is the responsibility of the user to choose reasonable passwords and not leave them written down anywhere, such as on their desk blotter or white board or pass them out to others.

The third matter is a paradigm of a different nature. This has to do with socially acceptable values. Namely, when I was brought up, I was taught about trespassing. If I went to someone's house and found the front door wide open, I—I don't really know of anyone who would walk in and look around. They would, instead, stand at the door, ring the doorbell, knock or call out. This type of responsibility or sense of morals has to be applied to the computer technology field.

Another area is research into methods of improving the safeguarding of information flow through technology should be pursued. One such project is the one of which I am the principal investigator of at SRI, which has to do with this type of technology. Our involvement has to do with developing and proving technologies that will absolutely assure that I will only have access to information in the computer system data base of which my need to know entitles me to, while prohibiting me from information I am not cleared or permitted to access. However, one must carefully weigh the value of increased security with the cost in user convenience and flexibility.

And lastly, explicit Federal and State criminal statutes should be enacted to allow a vehicle for vigorous prosecution, should it be warranted or desired by injured parties. These explicit laws would also hopefully act as a method of deterrence.

Now, let us not lull ourselves into a false sense of security. In general, unsanctioned computer system penetrations can be performed by idividuals who possess—who possess three basic access—aspects of computer knowlege: skill, access, and information.

Access can be defined as a terminal and modem. Skill can be defined as ingenuity or familiarity with computer systems, especially with the given system type that the penetration is directed toward. Information can be defined as dial-up phone numbers, network addresses, or other means of accessing a given computer system, perhaps even physical. Information can—also includes various methods, most likely in the form of bugs, that is, shortcomings, or features, an aspect inherent to the hardware or software design of the system which will permit the holder to circumvent the operating system security and protection mechanisms and, in effect, gain carte blanche access to the computer. Carte blanche can be defined as allowing the holder to override file security and protection considerations, in that you can read or alter any data or even change the nature of the computer operating system software itself.

In the good old days, such skill and information was not widely known. However, with the ever-increasing number of computer systems, both personal and mainframe alike, information and skill is spreading to an ever-increasing number of individuals and institutions. Unfortunately, not all the individuals are as scrupulous as they should be. Such instruments as pirate bulletin board systems are being used to disseminate this information on a nationwide, on-call, as-needed basis.

What does this mean? Up until now, most unsanctioned computer system penetrations have not been the high technological acts of chicanery the media has made them out to be. They were primarily performed by individuals who were as familiar with computer technology as, say, an auto enthusiast is what—is with what goes on underneath the hood of your car. The auto whiz has the breadth of knowledge necessary to hotwire a motor vehicle, just as your computer literate individual has the breadth necessary to perform a technological hotwire inside a computer system.

However, the current low to medium technological approaches to system penetrations are likely to change.

I define the technological levels as follows. High tech is defined as a new method of circumvention. High-tech methods are primarily invented by individuals or groups of individuals who have an indepth understanding of the desired technology the caper is directed against. Medium tech can be defined as an individual who has the same basic level of understanding as the high-tech guy, but uses the knowledge and perhaps fine tunes it a bit. The medium-tech guy is a knowledgeable user. The low-tech individual is just a user of the knowledge with little or no understanding of what is involved in making the technology perform its desired function.

In the not-too-distant future with higher stakes, increased levels of knowledge and other aspects better understood, I believe we will see a trend toward a more higher tech level system penetrations and circumventions. These capers will be harder to deter and detect.

The further development of formal specification and verification techniques, for both hardware and software, and associated technologies will permit the system developers, reviewers and the specifier himself to verify that his system specification is consistent with a given model of desired operation.

Recommendations. In conclusion, I would like to say that I believe the scale of the hacking problem is going to escalate dramatically as more of the technology makes its way into the mass market. There is no one easy solution to these problems. The directions that need to be taken are technological, ethical, moral, and social. Hopefully, an increased awareness of the vulnerability of our systems to penetration and circumvention will allow us to see the light in the form of solutions at the end of the tunnel. Hopefully, that light is not an oncoming train.

Thank you.

[The prepared statement of Mr. Goodfellow follows:]

Testimony by Geoffrey S. Goodfellow

Before the Subcommittee on Transportation, Aviation and Materials
on the subject of Telecommunications Security and Privacy.

22 September 1983

1. Introduction

My name is Geoffrey S. Goodfellow. I am primarily employed by the Computer Science Laboratory at SRI International, Menlo Park, California. For the past 10 years at SRI, I have been involved in research efforts related with packet switched computer network communication systems, protocols and security technologies. I have also been involved in various operating and sub-system development projects. Currently, my responsibilities include a position as Principle Investigator of SRI's involvement in a Department of Defense program aimed at developing and proving secure computer systems, that operate at different security levels and communicate via networks. A detailed biography of my career from 7th grade school where I discovered computers (which eventually lead to my permanent abandonment of the formal educational system during high school) to how I got to where I am today with no degrees or any type of equivalency to my name is included at the end of my testimony.

I am a coauthor of *the Hacker's Dictionary – A Guide to the World of Computer Wizards*, a new book being published this fall.

THE STATEMENTS INCLUDED HEREIN ARE MY OWN AND DO NOT NECESSARILY REPRESENT THOSE OF SRI INTERNATIONAL OR ANY CLIENTS OF SRI.

2. The Nature of Computer Hackers and Hacking.

The primary nature of a computer hacker can be defined as follows:

- A person who enjoys learning or knowing the details of computer systems and how to stretch their capabilities, as opposed to most users of computers, who prefer to learn or know only the minimum amount necessary in order to get their job done.

- One who programs computers enthusiastically, for the sheer fun of it, and gets a non professional amount of enjoyment out of using them.

- A person capable of appreciating the irony and beauty (i.e. 'hack value') of a program.

- A person who is good at programming quickly or is an expert on a particular program. *(This definition and the proceeding ones are correlated, and people who fit them congregate).*

Unfortunately, though, hacking has an unsavory faction to it:

- A malicious or inquisitive meddler (i.e. 'poacher') who tries to discover information by poking around. For example, a "password hacker" is one who tries, possibly by deceptive or illegal means, to discover other people's computer passwords. A "network hacker" is one who tries to learn about the computer network (possibly because he wants to interfere—one can tell the difference only by context, tone of voice and manner of approach).

Hackers of all factions, whether benign or of the unsavory flavor, consider themselves somewhat of an elite, though one to which new members are gladly welcome. Hacking is meritocracy based on ability. There is a certain self-satisfaction in identifying yourself as a hacker *(but if you claim to be one and are not, you'll quickly be labelled 'bogus').*

The hacker is intensely interested in technology and is a very inquisitive person. Many are social outcasts who don't enjoy the same things as most other kids their age. Hackers of the unsavory flavor are a very curious breed of individual – many can best be described as loners looking for someone to appreciate their talents. They know full well that what they're doing errs on the 'dark side *(of the force)'* – to coin a phrase. Unsavory hackers want to get caught so they can be given the appreciation they desire – and the process of getting caught adds an essence of thrill to their endeavor.

I would like to state for the record, that benign hackers, such as I, deplore the unsanctioned entry and subsequent rummaging of mainframe computer systems and networks. These types of activities are tarnishing the profession of hacking and giving it a bad name.

In the *Real World,* computer system organizations are generally run like totalitarian police states. This unfortunate reality fosters resentment in hackers and a desire to challenge the reverence of authority develops. As a result, the way hackers bring themselves to a system managers attention is via the medium they know and relate to best: a terminal and modem and your computer system. In most cases, the hacker wouldn't personally think of or know how to go about calling up the director of a computer system and offering his services to you as a bright young guy for the fear of reprisals or not being taken seriously. Instead, they choose to 'introduce' you to them by meddling with your computer system, cavalierly circumventing security and protection mechanisms, in order to satiate their hunger for knowledge and develop an understanding of how things work.

The organization will respond in kind by trying to 'plug the leak' of an intrusion into their system by erecting barriers. This type of reaction is precisely the wrong approach to take, because the hacker will notice the beefed-up defenses and see them as a further challenge of his prowess and ingenuity and legitimate users are subjected to greater inconvenience.

Instead, what an organization should do is try to befriend hackers which have penetrated their inner sanctums. The perspective that should be taken is one of *"Is it helpful or useful for you to do this?"* rather than *"Are you authorized to do this?"*. You must in effect come down to the hackers level and circulate among them. Show them that you appreciate their talents. If you ask them nonforeboding questions and take a genuine interest in what they're doing, most of the time you'll find they're more than happy to tell you exactly what it is they're looking for or interested in. The hacker wants to learn and you can be their guide/teacher. This is how I was dealt with by the firm that caught me during my unsavory hacking days in 1973 when I breached security on a large commercial timesharing network and many of its host computer systems. I was very much inspired by this method of catching and steering unsavory hackers towards more constructive use of their talents.

3. What Can and Should Be Done to Help Abate The Unsavory Hacking Problem?

From my own observations and inspections of systems and from what I have been reading in the press, I have come to the conclusion that computer site administrators are not taking reasonable and prudent measures to protect their computer systems from even the most casual methods of circumvention. A rather egregious example of this would be the installation of which the 414s allegedly logged into with username "test" and password "test". Usernames and passwords of this sort are not uncommon and sites which set up logins like this are just asking for a break in — just as someone who would leave a key in the lock on the front door of their house, complete with the WELCOME! mat out for all to see, invites the casual burglar.

The way I view 'reasonable and prudent' measures of protection from the *casual* penetration is by drawing a paradigm with the way DoD classified information is handled.

With respect to the handling and use of classified information, it is the responsibility of the organization to which you belong, in conformance with DoD guidelines, to provide you with rules and regulations in the handling of classified information. It is also the responsibility of your organization to provide you with a safe place (i.e. a vault) to store said information and to provide adequate safeguards (such as alarm systems, security personnel and patrols) to prevent unauthorized access.

The same methodology should be taken to heart by administrators of computer systems. It's their responsibility to provide reasonable and prudent measures to prevent unauthorized access attempts from gaining access to the system. This means a few very basic things like:

- Forcing users to choose reasonable passwords - not their spouse's name or their dog's name.
- Setting up proper modem controls on dial-up/remote access ports so that disconnection causes any jobs (or trojan horses left on the port) to be flushed and results in resetting the port to not-logged in status.
- Reporting incorrect password attempts to the system console or log file.
- Causing line disconnection after a few successively repeated incorrect password attempts.
- Using encrypted passwords, so it is not possible to compromise an entire systems password list when circumvention of a systems protection mechanisms is attained. This is analogous to the DoD's *compartmentalization* of information — so a breach in one area does not sacrifice security in all areas.

The second facet of the paradigm is the users' responsibility. I don't go out to lunch and leave my secrets sitting on my desk. I put them in a vault. And I don't go throwing them over the embassy walls. So it is the same for the computer system user. It is the users responsibility to choose reasonable passwords and not leave them written down anywhere, such as on their desk blotter or white board or to pass them out to others.

The third matter is a paradigm of a different nature. This has to do with socially acceptable values. Namely, when I was brought up, I was taught about trespassing. If I went to someone's house and found the front door is wide open, I don't really know of anyone who would walk right in and look around.

They would instead stand at the door, ring the doorbell or knock or call out. This type of responsibility or sense of morals has to be applied to the computer technology field.

Research into methods of improving the safeguarding of information flow through technology should be pursued. One such project is the one of which I am the Principle Investigator of at SRI, which has to do with this type of technology. Our involvement has to do with developing and proving technologies that will absolutely assure that I will only have access to information in a computer system database of which my clearance and my 'need to know' entitles me too, while prohibiting me from information I am not cleared or permitted to access. However, one must carefully weigh the value of increased security with the cost in user convenience and flexibility.

Explicit federal and state criminal statutes should be enacted to allow a vehicle for vigorous prosecution, should it be warranted or desired, by injured parties. These explicit laws would also hopefully act as a method of deterrence.

4. Let Us Not Lull Ourselves into a False Sense of Security.

In general unsanctioned computer system penetrations can be performed by individuals who possess three basic aspects of computer knowledge: access, skill and information.

Access can be defined as a terminal and modem. Skill can be defined as ingenuity or familiarity with computer systems, especially with the given system type that the penetration is directed towards. Information can be defined as dial-up phone numbers, network address or means of accessing a given computer system – perhaps even physical. Information can also include various methods, most likely in the form of 'bugs' (i.e. shortcomings) or 'features' (i.e. an aspect inherent to the hardware or software design of the system) which will permit the holder to circumvent the operating system security and protection mechanisms, and in effect gain *carte blanche* access to the computer. *Carte blanche* can be defined as allowing the holder to override file security and protection considerations, in that you can read or alter any data and even change the nature of the computer operating system software itself.

In the *good ol' days* such skill and information was not widely known. However, with the ever increasing number of computer systems, both personal and mainframe alike, information and skill is spreading to an ever increasing number of individuals and institutions. Unfortunately, not all of the individuals are as scrupulous as they should be. Such instruments as 'Pirate Bulletin Board' systems are being used to disseminate this information on a nationwide, on-call, as-needed basis.

What does this mean?

Up until now most unsanctioned computer system penetrations have not been the high technological acts of chicanery the media has made them out to be. They were primarily performed by individuals who were as familiar with computer technology as, say, an auto enthusiast is with what goes on under the hood of your car. The 'auto whiz' has the breadth of knowledge necessary to 'hot wire' a motor vehicle, just as your computer literate individual has the breadth to necessary to perform a technological 'hot wire' inside a computer system.

However, the current low to medium technological approaches to system penetrations are likely to change.

I define the technological levels as follows: *high tech* is defined as a new method of circumvention. High tech methods are primarily invented by individuals or a group of individuals who have an in depth understanding of the desired technology the caper is directed against. *Medium tech* can be defined as an individual who has the same basic level of understanding as the high tech guy, but uses the knowledge and perhaps fine tunes or refines it a bit (i.e. the medium tech individual is a knowledgeable user). The *low tech* individual is just a user of the knowledge with little or no understanding of what is involved in making the technology perform its desired function.

In the not to distant future with higher stakes, increased levels of knowledge and other aspects better understood, I believe we will see a trend towards a more 'higher tech' level of system penetrations and circumventions. These capers will be harder to detect and deter.

The further development of *formal specification* and *verification techniques* and associated technologies will permit the system developers, reviewers or specifier himself to verify that a given system specification is consistent with a given model of desired operation.

5. Recommendations

In conclusion, I would like to say that I believe the scale of the hacking problem is going to escalate dramatically as more of the technology makes its way into the mass market. There is no one easy solution to these problems. The directions that need to be taken are technological, ethical/moral and social. Hopefully an increased awareness of the vulnerability of our systems to penetration and circumvention will allow us to see the light, in the form of solutions, at the end of the tunnel. And hopefully that light, is not a train.

6. Biography *(The Making of a Hacker)*

My first experience with computers (and the world of 'hacking') manifested itself during my 7th grade school when I discovered a room full of teletypes connected to a computer system at Stanford University which offered Computer Assisted Instruction/drill programs.

Having discovered 'The Computer Room', I started arriving at school early each day to be able to play with them. I would also spend the lunch hour, recess and as long as I could after school in the computer room, as well.

Luckily, that summer I was permitted to hang-out at the Stanford facility which had the computer system that served our school and others. This allowed me the opportunity to interact with the system designers and learn how everything worked. At the facility, I quickly began to develop a keen interest in system-level software, such as the operating system and privileged type programs which only 'the wizards' could run or know the inner workings of. However, I did not let this fact keep me from learning about the system.

During the 8th grade, my parents wishing to contribute to their son's apparent avid absorption of computer technology, procured a used teletype machine and modem from a large time-sharing computer firm. I don't know how, but in the process, they managed to talk the firm out of 'free' account for after hours and weekend use. The firm then promptly forgot about me. After running the usual course of computer games, which quickly became quite boring, my attention turned towards the operating system and its protection mechanism, which I took delight in finding ways around. This of course, was noticed by the time-sharing company and one summer evening, after they were sure it was me inside their system, their vice president and district manager came knocking at our door, and in effect said, "gotcha!". The result of being caught was that I was hired for the summer to help them make their system more secure and plug the holes that I had uncovered in my wanderings.

While employed for the summer, 1973, I chanced to meet up with another summer hire who had done some work at NASA-AMES and had knowledge of a Department of Defense computer network, called the ARPANET, which linked_together computers all over the country at various research establishments, universities and military bases. My new-found friend passed me a dial-up number, and on a scrap of paper, wrote a few commands that would allow me to connect up to various systems on the network.

In these early days of the ARPANET (which pioneered packet switching technology, a method for allowing computers of different flavors and types to 'talk' to one-another), the majority of the computers had 'guest' accounts on them with purposefully obvious and published passwords. This was done in order to promote the free use of resources at other host systems and to let users of the network have a chance to explore, learn and use said systems.

Needless to say, this was a gold mine that no hacker, such as myself, could pass up. So I spent the better part of the summer learning and using as many different computer systems as possible, all over the country.

One of my favorite systems to use was the guest login account on a host called SRI-AI, a PDP-10 running the Tenex operating system, which belonged to the Stanford Research Institute's Artificial Intelligence Center. I thought it nice to have a system right in my very own home town. I made it a point to get to know the operations of this system as well as I could in hopes that perhaps someday I might have a login account of my own to use and it would be nice to be familiar with it in such an event.

Well, that day came when, as usual, I logged into the public guest account, and out popped a message of the form "Welcome to the SRI-AI computer public guest account. If you think you have a need for your own account, send a note (with the on-line electronic mail program, of course) to the system administrator, explaining your need."

Such an invitation was just to good to pass up and having my very own login account is something I had dreamed about. So, I took it upon myself to send a message saying I was a hacker who had been spending time on the public guest account learning about their system and wanted to have an increased level of access and login area of my own to store files. In return, I would freely help improve the systems capabilities thru my hacking.

After some initial trepidation on the part of the systems administrator was overcome, my account was granted. This allowed me to make SRI-AI my home base of network operations. I immediately proceeded to hack away to my heart's content, now that, in effect, I had become a legitimate network user.

After demonstrating my competence and some semblance of responsibility, I was granted system privileges (i.e. *carte blanche* access to all system resources). This permitted me to learn and develop a further understanding of the system.

So, I hung around SRI for about 9 months. I was given a building pass, so as to have physical as well as electronic (remote) access to the computer systems. This allowed me to come and go at odd hours, which are the hours hackers are best known to keep.

Then, there was an opening for a part-time weekend computer operator's job, and since I had demonstrated my competence, I was immediately hired for the position. I was now in my senior year of high school, and as a result of my increased access to computers, my grade average followed the typical hacker curve, i.e. down. until, two weeks into the final quarter of my senior year in high school, I dropped out, and became full-time at SRI. I have never returned to a classroom since the day I left school in 1974.

Mr. **Parker**. I'd like to just briefly comment by starting with my recommendations, and then just a couple of supporting comments.

First of all, I think it would be very useful if we had a national commission on information crime similar to the Privacy Protection Study Commission developed by Congress to study the privacy problem under the Privacy Act of 1974.

I call this privacy protection—I call the commission on information crime information crime rather than computer crime, because I think we should be focusing on the assets subject to loss rather than the instruments of causing that loss. In fact, ideally, I would like to see legislation focused more on information crime rather than on computer crime, because computer technology changes so rapidly, and I would hate to see this legislation become outmoded very quickly.

In the other hand, information crime is a new concept and, ideally speaking, it seems straightforward and simple, but practically, it may be quite complex.

I support Mr. Wyden's bill, H.R. 3075, and suggest that my recommendation is really an expansion of what he has proposed in his bill by having a national commission covering the whole subject of information crime and security rather than just for small business.

I also think in Mr. Wyden's bill, there is a very important concept, and that is of having a resource center available to business organizations to help them with their problems having to do with information crime, and also having to do with security advice. I would think that a department in which this might be focused would be the Department of Commerce, and that would give this the breadth of—of—of advice that would be most practical in—in—in this regard.

So the two functions, then, a national commission on information crime and security, and a resource center to provide this kind of information.

The National Bureau of Standards' Institute of Computer Sciences and Technology is already doing a very good job on this within the Federal Government. I'd like to see that expanded and that responsibility widened to provide it for the business community directly as well.

The privacy issue—I've made an analogy here with the Privacy Protection Study Commission. The privacy issue is really just a part of this information crime problem. And, therefore, I would like to say that certainly the issue that we are faced with now in dealing with information crime is far more important and a much broader subject now needing attention than the very narrow privacy issue was of almost 10 years ago.

A few words in support of this idea having to do with the nature of computer crime. Just briefly, to point out there are no valid statistics. We don't know how much computer crime there is. We don't know whether it's increasing or decreasing, from a statistical or numerical point of view. All the numbers that are floating around about computer crime are nonsense. They are not based on any valid studies. And, therefore, I think it's important to avoid using these numbers that keep floating around.

On the other hand, on a case-by-case study that we're doing at SRI, where we have over 1,100 cases in our research files, what we are finding is that the—that computer technology, through its concentration of assets in fragile form, and through its leverage that it gives the good guys, as well as that same computer leverage that gives leverage to the bad guys, is resulting in what I call escalation of business crime—not computer crime, but escalation of all kinds of business crime.

I believe that the more we use computers, the safer business and government becomes from the incidents of crime. I think there are fewer crimes the more we use computers, and that that will continue in the future.

On the other side of the coin, however, I believe that the loss per case is growing significantly. And the only evidence I can give you for that is on a case-by-case basis. We had in 1980 the largest funds transfer fraud in history, $10.2 million. In 1980, we had 257 people killed through criminal negligence in the programing of flight navigation computers.

Mr. GLICKMAN. What case is that, the airline crash you're talking about? Do you recall which airline it was?

Mr. PARKER. I don't recall which airline, but it happened in Antarctica, and it was an airline out of New Zealand.

Mr. GLICKMAN. Was it Air New Zealand?

Mr. PARKER. Yes.

Mr. GLICKMAN. I was just curious. Last week, this subcommittee had exact hearings on the issue of airline navigation in the wake of Korean 007. Nobody has yet alleged that that plane may have been criminally misprogramed. And I am just——

Mr. PARKER. Well—and again, there—you know, there are two sides to these things. I think that, most likely, the increasing use of computers for flight—air navigation has probably reduced the loss of life very significantly. But it's the one single case that can be very large that is the escalation problem.

In 1981, we had a $21.3 million bank embezzlement, the largest bank embezzlement in history. We had the largest securities fraud in history that same year, $53 million; the largest commodities fraud in that same year, $50 million; and last year, the largest inventory fraud, $67 million. These are record-breaking frauds and crimes brought about in various ways by the advancing use of technology. And so that's at least in partial support of my idea about the fact that we're facing an escalation in business crime today.

We're now facing new kinds of computer criminals as well. In the 13 years I've been studying computer crime, the computer criminal has been mostly the amateur white-collar criminal. We are now starting to see an increasing number of career criminals and organized crime getting into computer technology. And we're also seeing, as Jeff has described here, this new kind of problem, the malicious hacker problem, which is really an outgrowth of the phone freaks of the 1960's.

So it is nothing really new but it is an evolutionary thing of crime keeping up with the technology and crime using new technology. So we can anticipate in the future some probably startling events, as the technology continues to advance, we might not even imagine today.

I could foresee in the next 5 years, in fact, where the term "computer crime" will probably go away. That is because all business crime, all white collar crime, will be computer crime because it couldn't happen without an involvement one way or another, with computers.

And, again, that supports the idea that we really should be addressing the problem of information crime rather than computer crime. I am a strong supporter of Congressman Nelson's bill as well, computer crime bill. I think that it still needs further modification in a couple of areas. But the bill basically, I believe, is sound, and is an extremely important bill as part of the solution—not all, obviously, but part of the solution to the whole problem.

Now, going back to the system hacker problem, I think that's been covered and probably almost been beaten to death so far, so I don't have too much more to say about that except maybe just one point. And that is, in a table in my—in my testimony, I point out that this, this so-called innocent system hacking can be very serious indeed. And if you will note, just looking in the last 3 years, various cases of system hacking that have caused losses anywhere from $450, which is not very much, but several cases upward of $300,000 in the simple little cases of kids playing games in other people's computers.

And as Mr. McClary indicated from Los Alamos, it—the major loss is the loss of manpower of technical people having to deal with this kind of problem, ends up costing victims a very significant amount of money. So even though they may not have destroyed very much as far as tangible or intangible property, they can cause us a very large amount of loss in business and Government today.

Another aspect that was not covered here and that is very closely allied to hacking, that's the problem of the unauthorized copying of computer programs. There are various industry estimates that it is—amounts to 20 percent to 60 percent of all commercial computer program packages are unauthorized copies today with a gross violation of copyright and trade secret laws.

That is very closely allied to the—to the hacking problem, because there is a great overlap that hackers spend a great amount of their time, many of them in so-called software piracy, although I hate to use the term software piracy because it is software thievery, and the people who do it are thieves, not glorified pirates.

So I think we have to also take that aspect of the problem into account when we are looking at the hacking problem as well.

On the computer security side of the whole thing, a lot of that has also been covered and I don't want to—I don't want to repeat it. However, there is one point, and that is the role of the insurance industry.

The insurance industry has been a sleeping giant as far as taking its—its proper place and role in computer security. The insurance industry has taken an extremely role, and a proper one, in—in fire prevention and suppression. And it is only awakening now to its role in computer security, in information security, the broader term.

When we have premiums for insurance on information geared essentially to the amount of security in place, this is going to be a very important incentive for organizations to spend more money on security if they get a trade-off. And part of that by reduced premiums. And because we have such a tremendous leverage with security, that is, with proper security we reduce the risk of using computers of loss of information tremendously. But without adequate baseline of security, we have increased the risk of loss of information tremendously. That makes the insurance leverage in stimulating the use of security a very, very powerful in the field.

One last point, and that has to do with the national vulnerabilities issue. There has been considerable concern about how much damage could one single computer-related crime do to this country.

In Sweden, the Ministry of Defense conducted a study in which they concluded that the sovereignty of Sweden is currently at risk relative to one relatively simple attack involving their computer systems. Well, Sweden is not the United States.

The American Federation of Information Processing Societies in fact had a task group that looked at this problem. And I participated in that. The one conclusion was that today we don't think that there is a specific national vulnerability, that is, that the economy in some sense might collapse as a result of a single act involving computers primarily because of the resiliency of our system and of citizens in this country to respond to a national situation.

However, we concluded, also, that continued vigilance is extremely important because as we become more and more dependent on computers, then we could reach a state in which the risk of a national calamity could be unmanageable and unacceptable to us.

So, I believe that this very important issue of national vulnerabilities, coupled with this hacker problem that we are dealing with today, the problem of the proprietary ownership and protection of computer programs which is in danger of causing massive harm to the—to the billion-dollar-a-year software industry, the increasing incidence of career criminals and organized crime apparently moving into this area of technology leads me to believe that we do need the strong support that the bills like Congressman Wyden and Nelson are proposing. And my recommendation for a national commission to study this problem the way we had the privacy problem, very important.

[The prepared statement of Mr. Parker follows:]

TESTIMONY BY DONN B. PARKER
Telecommunications Security and Privacy

Before the Subcommittee on Transportation, Aviation and Materials, Committee on Science and Technology, United States House of Representatives

September 26, 1983

Introduction

My name is Donn B. Parker. I have worked in the fields of computer programming and computer systems management for 30 years. For the past 13 years of my career, I have been a researcher and consultant specializing in the computer crime problem and computer security. I have a Master of Arts degree in mathematics from the University of California at Berkeley. I am a Senior Management Systems Consultant in the Information Systems Management Department at SRI International, Menlo Park, California. The statements included herein are my own and do not necessarily represent those of SRI International or any clients of SRI. In this testimony it is my practice not to identify the names of any victims or perpetrators of crimes because they have suffered enough from embarrassment in public exposure and deserve anonimity in their attempt to recover.

My published works include the definitive book on computer crime, Crime by Computer, in 1976; a new book Fighting Computer Crime, was recently published. In addition, I have written two books for the professional audience, Computer Security Management and Ethical Conflicts in Computer Science and Technology. My SRI associate, Ms. Susan Nycum, a leading lawyer in computer law, and I produced the definitive manual on computer crime investigation and prosecution, Criminal Justice Resource Manual on Computer Crime, and a new report, Computer Security Techniques, for the Bureau of Justice Statistics of the U.S. Department of Justice. I am project leader for a new study for the Bureau of Justice Statistics at SRI to enumerate all cases charged under the 21 state computer crime statutes and report on the unauthorized computer access and computer program theft problems.

Recommendations

Both the incidence of, and the loss from, computer crime appear to be growing at a fast rate and are receiving great attention in the news media. Yet the problem and its solutions seem to be little understood by either victims, potential victims, management, teachers, researchers, the criminal justice system, or legislators. This is similar to the situation concerning privacy in the mid 1970s, when Congress established the National Commission on the Rights of Privacy as a result of the impact of computer technology on the confidentiality of personal information. Therefore, a similar action seems appropriate to deal with this similar but broader, and more serious, problem.

I propose that Congress appoint a National Commission on Information Crime with a charter functionally similar to the former Privacy Protection Study Commission created by the Privacy Act of 1974. I choose the words information crime instead of computer crime in the title because there should be a broader context of inquiry about crime in the information age, not inhibited by a specific technology that is so rapidly changing. The inquiry should be focused on the assets at risk rather than the instruments of loss. The Commission could then scale and scope its inquiry as its findings indicate. The results of the effort could include: establishment of official definitions; characterization of the problems and recommended actions including legislation and control efforts by a wide range of businesses, organizations, and institutions; as well as establishing values throughout society to deal with the new problems.

This recommendation is similar, in part, to one provision in a current House bill, H.R. 3075, the "Small Business Computer Crime Prevention Act," introduced by Representative Ron Wyden, which calls for a Small Business Computer Crime and Security Task Force. My recommendation would widen the scope of such an effort to all victims of information crime.

In action similar to the second part of Mr. Wyden's bill, a national resource center could be established in the Department of Commerce to provide information and advice on information crime and security. The Center would rely heavily on the excellent work on computer security being done by the National Bureau of Standards, Institute for Computer Sciences and Technology and on computer crime research being done by the Bureau of Justice Statistics in the Department of Justice. The Center could also draw on work being done on computer security by the Department of Defense, the General Accounting Office and among the Departments' Inspectors General, as well as their contractors.

A national information strategy is needed. A group of computer and telecommunications industry leaders are proposing a Temporary National Information Committee to be funded by private industry with the cooperation of the Federal Government. While its scope would cover all the data gathering and dissemination aspects of the computer and telecommunications revolution, it would encompass security.

While information crime includes the violation of privacy, it is a far larger problem for society than the privacy issue. Therefore, it deserves at least as much attention even though it may not be as intellectually stimulating and challenging and may not carry invasion of privacy's personal imperative.

The Nature of Computer Crime

As background in support of the above recommendations, I would like to offer the following information. Computer crime is defined here as any crime in which the criminal required special knowledge of computers or data communications for its perpetration.

There are no valid statistics on the size of the computer crime problem. We only know the nature of the problem based on a case-by-case, empirical analysis of known and reported cases that represent a limited collection of information. For example, most of the 1100 cases in our research files at SRI were accidentally discovered and reported in spite of the reluctance of the victims to reveal their losses. Therefore, we wonder how many really smart perpetrators don't get caught, detected, or reported. I conjecture that there is an escalation of all kinds of business and white collar crime, not only computer crime, caused by the increasing use and dependence on computers and data communications. By escalation I mean that the frequency of crimes is diminishing while the size of each loss is increasing.

Based on reported cases in just the last few years, the losses seem to be breaking records as indicated in the following cases:

o	1980	$1.2 million	The largest funds transfer fraud.
o	1980	257 people killed	One of the severest airliner crashes caused by criminal negligence in programming a flight navigation computer
o	1981	$21.3 million	The largest bank embezzlement
o	1981	$53 million	The largest securities fraud
o	1981	$50 million	The largest commodities fraud
o	1982	$67 million	The largest inventory fraud

These massive crimes were all facilitated by two facts: (1) A concentration of information assets was by being stored, processed, communicated and outputted by computers and telecommunications systems, and (2) these assets were removed from direct human view or evaluation and safeguarding.

As far as can be determined from reported crime cases, eavesdropping on data communications is not yet a problem in the use of computers. Only 3 cases are known to have occurred, probably because there are so many easier, less costly, and safer ways for the perpetrators to obtain or modify data. This is probably why businesses are not yet willing to install cryptographic protection (the ideal safeguard from such crime). They have too many other greater vulnerabilities to deal with first.

New kinds of criminals are appearing in computer crime; past crimes have been committed mostly by amateur white collar perpetrators in positions of trust. There seems to be an increase recently in career criminals and organized crime activity. The most recent and visible problem is an epidemic of malicious computer and communications accessing as an outgrowth of attacking telephone systems (phone phreaking) in the 1960s. This problem is treated in a separate section below. Closely associated with this problem is the unauthorized copying and theft of computer programs that seems to be challenging the viability of the commercial computer program market. This problem is commonly known as software piracy and is also treated below.

Computer and Communications Security

The subject of computer and communications security is rapidly maturing. We now know most of the vulnerabilities and have identified and developed cost effective controls that reduce, to acceptable levels, the risk of loss in the technologies currently used in business. Most reported losses now occur in environments where there is an incredible lack of security, and where well known, practical safeguards would have prevented or reduced the losses. It must be noted that total security is not practical, and there are no adequately secure commercially available computers or communications. However, a combination of programmed, hardware, physical, procedural, and most importantly human controls can provide adequate security today. The critical problem now is sufficiently motivating management and persons in positions of trust to use and support such controls.

Unfortunately, computer and communications security has been mostly in the hands of technologists who tend to seek and advance technological solutions to problems. However, the problem is primarily a people problem, and the solutions must be a combination of both technical and human controls. Therefore, the greatest need today is to advance the human controls to the same level as the technical ones. By human controls I mean such procedures as establishing business policies supporting security, codes of conduct, annual employee security briefings, vetting of employees in positions of trust, employee performance and salary reviews that evaluate security performance, confidential problem-solving services for employees, and use of informant intelligence-gathering techniques.

Another mostly overlooked factor in risk reduction is insurance. The insurance industry has been a sleeping giant in the information age, but is now awakening to the huge potential market for information insurance and loss reduction. Policies that protect against loss during electronic data processing, loss of electronic products, or loss from computer crime are currently available. However, great improvements are needed including premium discounts for installed safeguards. This will provide great incentive for computer owners to improve security.

The Computer Hacker Problem

Computer hackers are hobbyists with intense interest in exploring the capabilities of computers and communications and causing these systems to perform to their limits. They are also called system hackers, or compulsive programmers, and often constitute subcultures within schools, computer clubs, and technological work environments. Hackers exhibit a spectrum of behavior from benign to malicious. Malicious hacking consists mostly of unauthorized access from a terminal connected by telephone to a dial-up access computer owned by another party, followed in some cases by various acts of vandalism such as destroying or contaminating data or use of computer service.

Hackers generally attempt to rationalize their activities by indicating the great educational value and satisfaction of benign intellectual curiosity and experiment. Their definition of malicious hacking is quite different from that of the victims. Malice means to cause harm without legal justification or excuse or intent to commit an unlawful act. Malicious mischief is willful, wanton or reckless damage to, or destruction of, another's property. These latter definitions provide appropriate descriptions of malicious hacking from victims' perspective.

Malicious hackers rationalize that entering another's computer electronically without invitation is not the same as physically entering another's private domain of office or home, that erasing or contaminating computer-stored data is not destruction of property, or that use of another's computer services is not theft of services. Small differences in ethical issues can be argued as being difficult for juveniles to distinguish or be concerned about; therefore, potential victims of hacking need to exceed normal precautions by making the criminality of these acts exceptionally clear.

Consideration of the hacking problem requires measuring, or at least estimating, its size. Comments range from epidemic to minor annoyance, but no valid estimates of incidence, frequency, loss, or numbers of malicious hackers have been made since there is no mechanism for collecting data and no survey has been done. However, a limited estimate for the country based on one knowledgeable hacker's estimate of 100 hard-core hackers for the Detroit metropolitan area, and easily identified 128 pirate bulletin boards across the country, indicates that there are probably thousands of hackers attacking private computer systems.

A hard-core hacker is defined as an individual who attempts to gain unauthorized access to computers on a sustained, long-term basis and is recognized by other hackers for his skills, knowledge and daring. The number probably varies with circumstances such as public visibility and hacking opportunities. For example, the movie Wargames probably caused a significant increase in hacking as did the making of heroes of the Milwaukee 414 Gang members in national news media.

For example, the September 5, 1983 issue of Newsweek made a hero out of a computer hacker on its cover and 45% of the cover story (70 of 156 column-inches) was uncritical, if not admiring of the Milwaukee 414 gang. The article then ends with: "Deterrence is not going to be easy as long as the media glorify hackers like the 414s as the Robin Hoods of the information age."

Arrests and convictions probably have an effect too difficult to estimate because they tend to suppress the more timid and law-abiding while encouraging the more bold and amoral.

The size of the problem is increasing as terminals, modems, and microcomputers become more available. Richard J. Matlack, President of Infocorp, a marketing research firm, estimates that there are about 600,000 computers used in homes, and 120,000 to 180,000 of them are equipped with modems used to gain access through telephones. Another contribution to the size is an increasing number of juveniles learning the technology; propagation of capabilities, and encouragement of younger neophytes by older hackers is common. Many hackers claim they were taught and/or encouraged by older juveniles or adults. There is general advice, often heard, to engage in hacking before reaching the age of exposure to adult criminal prosecution. Particularly virulent pirate boards with new hacking intelligence also probably stimulate activity.

Some types of losses are known on a case-by-case basis. They consist mostly of:

- o Destroyed or contaminated data files and computer programs.
- o Use of computer or telecommunication services or denial of use of such services.
- o Theft of copies of programs or data for personal or associates' use or gain.
- o Modification of programs or data for personal or associates' gain.

Table 1 provides a summary of recent cases indicating victims' estimates of losses. Note that victim names are not shown but are available from Donn B. Parker for verification purposes.

Table 1

Losses in Recent Cases

Year	Type of Loss	Amount
81	Denial of service and staff time	$260,000
81	Theft of equipment and telephone services	$300,000
82	Denial of service and loss of business	$100,000
82	Loss of data and programs and staff time	$ 25,000
83	Restoration of data files and staff time	$ 450
83	Credit card data used to order products	$ 50,000

Solutions to the hacker problem might be achieved in three areas.

First, adoption of specific criminal statutes and vigorous prosecution as deterrents are basic requirements. Many of the 21 state computer crime statutes explicitly identify unauthorized access as a crime. The current Federal bill, H.R. 3970 "Federal Computer Systems Protection Act," sponsored by Mr. Bill Nelson, can provide necessary protection on an interstate basis. However, it has technical flaws and should be revised.

Second, well known controls should be used by host computer owners. This will provide at least a confrontation level of security equivalent to a locked door. The ethical and social values applicable to entry to private, physical domains such as homes or offices may not be seen by immature or less responsible people as clearly or directly applicable to private, electronic domains such as computers. Therefore, it is prudent for host computer systems to provide the equivalent of "No Trespassing Except to Authorized Persons" signs to confront anybody attempting access to the systems.

Third, and most difficult, is an effort to change the values of hackers and provide them with constructive and attractive outlets for their interests and energy. This will have little effect on many hard-core hackers who have other deep problems, but many of the more benign and reasonable ones can be saved. I answer those who scoff at attempting to change the application of ethical values by suggesting that it would be irresponsible of us not to try. Value changing could be done by professional, trade, and educational associations with the cooperation and support of the victims of hacking and suppliers of products that might be used by hackers.

Computer Program Theft

The unauthorized copying of computer programs resulting in displaced sales and unauthorized sale of copies is commonly called software piracy, and those who do it are called pirates. Unfortunately, this terminology lends glamour and semilegitimacy to the practice. The people who do it should be called thieves. It is estimated by various industry sources that 20% to 60% of all commercial program packages in use are illegal copies. This would represent a loss of $200 million to $600 million in the $1 billion annual sales industry-wide. However, no valid statistical survey has been conducted. This problem is closely associated with the hacking problem because of the significant overlap of perpetrators. Therefore, the solutions are similar and should be designed to deal with both problems.

National Vulnerabilities

There is considerable speculation about how large a single computer crime could be, especially after a Swedish Ministry of Defense study concluded that Sweden is vulnerable to national collapse from a computer crime because of increasing dependence on computers and telecommunications.

A task group was assembled by the American Federation of Information Processing Societies to study the vulnerability of the United States. After considering a wide array of possible loss scenarios, it was concluded that no single attack, short of war, could result in national collapse, even though great damage could be done. The resiliency of society to respond in positive ways and recover was the most significant reason for the conclusion. The task group warned that increasing dependence on computers and telecommunications requires continuing vigilence to preclude future problems that might arise. There are respected professionals in the computer and telecommunications field who do not agree with the conclusions and believe this country has already reached a critical stage of vulnerability. I believe that this important issue requires more study, which should be conducted by a Congressional National Commission.

Mr. GLICKMAN. Well, thank you both for excellent testimony. And I am going to try to get as much covered in mine as quickly as possible so the other gentlemen can ask their questions.

The computer revolution, the information revolution, causes me to have great concern whether we in the civilized world have lost control. I mean, are we the modern-day Dr. Frankensteins in what we have created? And is there really any way to control through proper security and vigilance a situation where ultimately we will not be able to put our finger on what the problem is; we will not be able to find out if, in fact, that logic bomb exists within a computer and that—and that all the steps we are taking will be just patchwork steps. I become more and more concerned that as technology advances, as the silicon chip becomes even more sophisticated, that the vigilance will not be able to deal with the problems.

Mr. PARKER. Well, we're—we're facing increasing risks in—in atomic energy, in the nuclear problem. And I think what we have here is something quite similar to that. I believe that computer security is advancing very rapidly and at least is currently keeping up the technology and with the value of information that we are currently storing in our systems and squeezing through telephone lines.

The problem is getting the potential victims to use the controls that we already know about and there are many extremely low-cost, very powerful controls. The problem is not solved as a technological problem. That's only part of the solution. It's a people problem. Computers don't commit crimes or make errors, only people can do that. But through a combination of technological controls, physical controls, operational procedural, the human controls that go along with that; for the first time in history I believe we have an opportunity to reduce crime and to make business and Government far safer than they ever were in previous manual systems.

And I think we ought to be taking advantage of that by bringing national attention to the fact that we do have adequate controls. It is a matter of using what we have. And there's always the risk—a computer program is unpredictable basically—but there is a lot of research going on that—that I think Mr. Walker will talk about after our testimony, and it is making very good progress.

Mr. GLICKMAN. Well, let me ask you. I asked this of the previous witness, I said, what if the 414 group have programed something in there that is to take effect triggered upon a later happening, or will happen as of a certain period of time—again, so to speak, the logic bomb issue, I said, will you know about it? He says, no, not really. I said, you mean there is no way to find out if something has been improperly or illegally programed into that system, there is no way to get a bibliography on it? And you heard his answer, I think. That causes me very great concern.

Mr. PARKER. What you are talking about, however, is absolute security. And we live in a world of risk. We live with risk, and we accept risk; and with a big enough hammer you can break anything. And, therefore, I think that, as I said, we are making progress. And through research, I think we are going to find ways not of eliminating the logic bomb problem, the Trojan horse problem, the salami attacks, asynchronist attacks, and so on, but I think we can reduce the likelihood that those things would happen in very serious ways to some reasonable level that we can live with. Like a nuclear reactor, I think you can reduce the risk of using a nuclear reactor to some reasonable level—the same thing with computers.

Mr. GLICKMAN. Well, there was a famous case involving a Judge Cardozo. He was a very famous legal leader juris—man of jurisprudence who defined negligence, the risk to be perceived that finds the duty to be obeyed. And I guess my concern here is that the nature of the risk, as you point out, may be so very significant, although small in terms of possibility, but when it happened it would be very significant that it does require these incredibly significant and detailed ways to try and avoid that kind of risk.

Let me get to the issue of privacy for a minute. It seems to me that computer technology has carried us to communication and information advancements that we never thought possible. But it looks to me like it's made stealing information a science and privacy an illusion.

Now, can you today say to us that there are the techniques available to protect the bank customer, the Master Charge customer, the person dependent upon keeping his or her records reasonably secure from other people using that information?

Mr. PARKER. Personal information stored in a computer system, I believe inherently is more secure than that same information stored in manila folders in locked file cabinets. I also believe that if the controls that are routine today, that we have available today, are applied—and they are being applied in many organizations today—increases our personal privacy very significantly. Therefore, I conclude the more we use computers, the more personal information we put into computers where we can control it to a far greater degree than we could in manual systems is increasing privacy by being able to enforce the rules of confidentiality that we were never able to do in a manual human environment.

Mr. **Glickman**. But that, of course, again relies upon the kind of backup systems that have a human component in them to insure they are working correctly.

What I fear is we could get into this country is backup on computer which is backed up on computer which is backed up on computer, and you are too far away in a human sense to either know that the problem is happening or deal with it once its happened. And I guess that goes for the basic issue of research and trying to devise systems that have the appropriate human machine interfaced there.

Let me ask you a question about the issue of national security. In The New York Times yesterday there was a story about computer security that says that the Defense Department, once confident that its computers were virtually impregnable, have become increasingly concerned about their future security.

And they talk about there have been surreptitious entries of computers have evolved to the point that exceedingly subtle changes in a computer's controlling program can snatch data without directly penetrating the computer's defense mechanisms. They talk about the amount of secret information that's going into computers.

Do you have any independent knowledge of these particular incidents that I am talking about?

Mr. **Parker**. No, I don't. And if I did, I wouldn't be able to talk about it. I—I don't think we are really in a position where we could talk about that. And I—frankly, I think that, that we're—part of security is keeping that kind of information confidential. And so I really think that's not the place to do that.

My only comment on this is that in viewing the Department of Defense from the outside—and I am not involved in that kind of work—I have a lot of confidence that with the effort that's being poured in security within the Department of Defense and the recognition of the live real enemy with unlimited resources results in extremely high level degree of security within the Department of Defense in the use of computers. And, in fact, most of what we have in security today in the business community came from and was developed within the military, and we can see things being developed in the military today that will be out being used in business tomorrow.

Mr. **Glickman**. OK. Actually, this area involves a lot of—involves going beyond just the computer issue. We talked about some of the ability to obtain from mag—you know, electromagnetics signals or noncomputer information capabilities. But I appreciate your comments on that.

I would ask you, and perhaps Mr. Goodfellow, will changing of passwords be an adequate countermeasure, or will hackers just get more creative in their efforts to break in?

Mr. Goodfellow. More creative, most definitely. That's what I wanted to—that's why I attempted to address in my later part—portion of my testimony was that the password is not enough. There are multiple levels of—of responsibility that you have to employ to make computer systems secure. And there is normally such as things as system password that would allow you to have global access to all data within a computer system.

But there are virtually unlimited user—normal user accounts who have a restricted access. But due to the computer technology today and its—in its inherent design, there isn't a computer system that's out there on the market today that, by being able to log into one of these mirror mortal accounts with some little chicanery under the fingertips of a knowledgeable person about that computer system can gain that systemwide access.

Mr. Parker. In one example, a group of high school students attacked their high school computer system. And the way they went about it was that they spent hundreds of hours simply monitoring the computer until one of the maintenance engineers forgot to resecure a file he was using and left it unsecure.

So no matter what you do technologically, it still comes back down to the people involved in positions of trust. And if an error is going to be made, it's not going to be the computer, it's going to be a person. And a system that is technologically secure today could have one small change made in it, an authorized change, and tomorrow the system is no longer secure.

Mr. Glickman. But again, as you point out, the problem comes in as we depend more and more upon sophisticated methods of storing information while the risk may be smaller, if in fact there's a jeopardy occurs, it may be a gigantic jeopardy.

Mr. Parker. That's the escalation problem?

Mr. Glickman. Yes.

Let me ask you this, Mr. Goodfellow, are—is there a hackers organization and association here in—a lobbyist group? I mean, how do you—not you, because you're not a hacker. But how do hackers talk to each other?

Mr. Goodfellow. Well, actually I do consider myself a hacker, but not a malicious or unsavory hacker—

Mr. Glickman. OK.

Mr. Goodfellow [continuing]. Because I—I do enjoy using computers enthusiastically and I hope I will for some time.

Mr. Glickman. Is there a hackers organization?

Mr. Goodfellow. No. There is no formal hackers organization that I know of but there are—are methods on various computer networks and private bulletin board systems to allow hackers to—to congregate sort of informally.

Mr. Glickman. There's no formal hackers magazine or anything where you can pick up the tricks of the trade?

Mr. Goodfellow. No.

Mr. Glickman. Are there examples of computer hacking for profit that you are aware of?

Mr. Goodfellow. You would mean—you mean the unsanctioned entry of computer systems?

Mr. Glickman. Yes.

Mr. GOODFELLOW. Well, not that I'm aware of. But it's my opinion in the future, and I was paid a visit by some of the Office of Special Investigations of the Air Force on this exact concern of theirs. In that—in the future what they were concerned about was sort of a type of an electronic Messiah, a charismatic figure being able to rally the unsavory hacker forces together, and in effect direct them towards the penetration—organized penetration—of computer systems.

No sooner did these officers come visit me and discuss this problem, that I discovered it 3 days later, this is going to be the plot for the follow-on movie to War Games that is currently in the script writing stage now.

Mr. GLICKMAN. You mean electronic Messiah, kind of like a cult leader——

Mr. GOODFELLOW. Yes.

Mr. GLICKMAN [continuing]. Who may decide to get his folks together by use of the computer—a 21st century Adolf Hitler then?

Mr. GOODFELLOW. Yes; a—on that, precisely.

Mr. PARKER. I—we do have some cases of hacking for profit. In one college, for example, the hackers were selling grade changing. And in another case, hackers were using their hacking capabilities to steal copies of copyrighted programs from their victims and then turning around and—and pirating, or selling those programs for profit.

Mr. GLICKMAN. Do you think that's widespread?

Mr. PARKER. We have no idea. There's been no study of this.

I am currently engaged in a project for the U.S. Department of Justice—Bureau of Justice Statistics—in which we are studying that problem right now. And we are also looking at the experience of prosecution under the 21-State computer crime laws. The results of that were—should be finished by the end of this year.

Mr. GLICKMAN. Thank you.

Let's see, Mr. Nelson.

Mr. NELSON. Thank you, Mr. Chairman.

Mr. Chairman, I would note that Donn Parker, for the record, I've known over the last 6 years, and it was primarily his input that helped us in the drafting of legislation that became the first computer crime law in the Nation under which Florida has just recently had a very successful prosecution. And you might be interested to know, Donn, that in talking with the State attorney, who did the prosecution in Miami, they said that the bill and its legislative intent was very significant in helping them suggest jury instructions to the judge, and that they were very pleased with its overall content. So, my thanks to you.

Let me ask you about the 20 States that since followed Florida. Have you seen these first tottering efforts of prosecution under those laws? Are they still afraid to approach them because of challenges by constitutional challenges, and so forth?

Mr. PARKER. Well, we are just starting that part of the study for the Bureau of Justice Statistics right now so I don't have a fuller—complete answers.

But I have been made to understand that any new law, a prosecutor is somewhat hesitant to use it if it's untested. And, therefore, there's a lag of time between their adoption and when they are really used significantly. And I think we've had as a result the slow start that you identify. But once started, then I think we will see a rapid increase in the use.

In California, I would guess that we've had on the order or at least 15 to 20 cases prosecuted. Colorado has probably had many more than that because they happen to have a broader computer crime law than California does.

But there are many of the other States that have had no experience in prosecution with these laws yet. But as I say, I think once it starts rolling it will increase.

Mr. NELSON. As you stated earlier, one of the problems is trying to identify what are the specific crimes all over the Nation—people are not forthcoming, rushing to us with information about this; in many cases because they are embarrassed that that particular criminal act occurred in their corporation or their area of responsibility.

What would be your answer to the people who say, well, you've got to show us evidence of widespread criminal uses of computer in order for us to want to endorse the concept that something must be done? What's your response to that?

Mr. PARKER. Well, first, I think that there are enough significant cases to point out an existence theorem, if you will, that the problem is there and it really is a serious problem. When you've got a securities fraud of $53 million, one simple fraud, commodities fraud of similar size, that, in and of itself, ought to be enough to draw attention to the possibility of the need for a law.

I think there has been probably less justification for other laws that have been adopted than the justification we just currently have now. But that was one of the reasons for my suggestion that a commission be developed that would hold hearings around the country and draw out this information from different parts of the country that might otherwise be difficult to find.

We are just not going to get good statistics on this. No one has ever gotten any good statistics on white collar crime. And I just don't think we are going to get really valid statistics but we are going to chip away at it. For instance, we will have this record of prosecutions under computer crime laws. And so I think we have to look at the small amount of experience that we know about and then by reason show why there is most likely a lot of it that is never reported.

Mr. NELSON. I wanted to ask your associate, Mr. Goodfellow, as a hacker, I noted that you think that there is a result of deterrence where there would be a State or a Federal criminal statute.

Could you elaborate on that?

Mr. GOODFELLOW. Absolutely. What I think is going to be needed is going to be some sensationalistic prosecution cases where some examples are—are made, and this might—might lay the groundwork as a deterrence that would hopefully have people think twice about—before they would go in and trash someone's computer system.

Mr. NELSON. Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you.

Mr. Wyden.

Mr. **Wyden**. Mr. Chairman, very briefly just a quick comment and then some questions. I would hope that in the Congress and in the private sector we certainly wouldn't glorify this concept of the electronic Messiah. It strikes me that we probably ought to call it for what it is, and that's more like an electronic Fagan. And I think in particular we need to do everything we can, particularly with the young people and with the movies coming out, to call this for what it is and not—and not glorify it.

What question for you, Donn—and both of you have just been superb witnesses. I have continually said that Donn Parker and Louise Becker of the Congressional Research Service really are mentors in the field for those of us in the Congress who have been active in this issue, and both of you have been superb this morning, as you usually are. And I wanted to ask you, Donn, about one thing you and I have talked about, and that's this kind of, I guess you could call it hackers product that was perpetrated on you when your most recent book came out. For those in the audience it talks about Mr. Parker's book, calls it, the book's title is "Fighting Computer Crime," and "the libelous pig dog author, a self-acclaimed expert, includes certain items which look as if they were downloaded using some sort of terminal."

Then it recommends, "Go to your local bookstore, pick up (read steal a copy of the book). I wouldn't support the bum, would you? I mean, anybody who would write that Susan Thunder was a hooker."

And it just goes on and on and on, signed, "Your friendly neighborhood freak, Milo Phonebill."

Where in the world did this come from and how could something like this get out around the country when it shows, in my estimation, a certain amount of gall to try to perpetrate this kind of thing on someone who is an expert in the computer crime field?

Mr. **Parker**. That review has probably sold a lot of books for me. It's typical of the kind of stuff we find in pirate bulletin boards. And you will notice some of the foul language that's used there and in it—it characterizes the—the immature minds of these kids. But that's the point that is really very dangerous, and that is we are putting into the hands of these immature people who write that kind of junk in their bulletin boards to one another. We are putting into their hands extremely powerful instruments. I mean, you don't give a child an airplane and go say, see if you can fly it. You give them all kinds of tests; they have to study the laws; they have to know the etiquette involved in flying airplanes; and they are licensed before they can use such a powerful tool.

I'm not saying that we should license kids before we let them use computers, but they certainly need this dose of ethics that you earlier mentioned before they are given a dose of the technology.

Mr. **Wyden**. Mr. Chairman, although I'm not a member of the committee, I would ask unanimous consent that this be made a part of the record.

Mr. **Glickman**. Without objection, it will be part of the record.

Mr. **Wyden**. I thank the gentleman.

Just two other questions for you, Mr. Parker, very briefly.

Do you—do you think the top management in the American business community is getting the message now? Are they coming to be aware of what a significant risk this is? I think you said it very well when you suggested that in the next few years computer crime isn't going to really exist as a concept. It is going to be information crime or simply business crime because all the crimes, for the most part, are going to be committed with a computer.

Is the business community getting the message? I've had business people tell me point blank, "Congressman, I think that what we ought to do is lock our top management in the board room and force them to stay there until we come up, you know, with a solution."

Now, do you get the feeling that other businesses are taking it that seriously? Are they getting the message?

Mr. **Parker**. Well, part of my work is consultant in computer security for top management in helping them develop security. And ever since the—the movie and the 414 gang, and so on, our phone has been ringing off the hook because top management cannot fail today to understand their vulnerabilities. And I would almost say any business today is still suffering from hacker attacks, probably deserves it. Not that I am endorsing anything that the hackers do in that regard but the point is I do think that management today, what they read in the magazines and in the journals that top management reads, they cannot help but read and know—and I am getting more and more calls from auditors and from security managers saying the board of directors, or chief executive officer, called me today and said what are you doing about all those things I'm reading about in the Wall Street Journal and New York Times, Newsweek, and so on?

And so I think that War Games, while it may be stimulating a lot of kids to do more of this kind of stuff, has probably had a very positive effect in warning management about their vulnerabilities.

Mr. **Wyden**. One other question. The gracious chairman has his gavel in his hand and I want to be quick.

And, by the way, your last point hitting right on target, I think we all understand people in this country have a constitutional right to do things that are bad for them. And no matter how many laws we pass, that's got to be respected. And if after all of this, people still don't want to secure their systems, there isn't that much we can do.

You called the insurance industry a sleeping giant and that it was finally beginning to wake up. How so? I haven't heard anything, for example, from the National Association of Insurance Commissioners, which strikes me as an ideal forum to catalyze some action in the insurance industry.

What manifestations have produced you to say that the insurance industry is starting to wake up because I think if they do, there's something in this for everybody—the chance to get a lower premium, the chance to lower insurance costs. That seems to be the ideal trigger to really get people serious. And maybe you could elaborate a little bit.

Mr. **Parker**. My comment is based on the new insurance products that are now on the market. EDP insurance has broadened and become very comprehensive. It has gradually moved from insuring the computer to insuring the media, the tapes and discs, and now it's moving to insuring the actual informations stored on the tapes and discs.

Also, we see it in the computer crime insurance that is now available that provides fidelity insurance and also insurance for crime from external sources. And we also see it in the electronic products insurance, that provides liability insurance, a theft of product insurance. And so it's a very much of a product oriented.

And the reason you haven't seen anything coming from the industry itself, is probably because this area is such a highly competitive area and is new that it hasn't really worked its way into the industry trade associations yet. But it soon will.

Mr. **Wyden**. Very good. And, again, I thank you for really a superb performance here this morning.

I thank the chairman.

Mr. **Glickman**. Thank you, Mr. Parker, and I hope you will continue your work.

Our last witness is Mr. Stephen Walker, President of Trusted Information Systems, Inc., Glenwood, Md.

It is a pleasure having you, Mr. Parker, appreciate your testimony. Your entire statement will appear in the records so if you want to summarize it, that would be fine with us.

STATEMENT OF STEPHEN T. WALKER, PRESIDENT, TRUSTED INFORMATION SYSTEMS, INC., INFORMATION SYSTEMS TELECOMMUNICATIONS, GLENWOOD, MD.

Mr. **Walker**. Thank you very much. I really appreciate the opportunity to be here. As my testimony states, I am now the president of Trusted Information Systems, Inc., which is a company recently formed essentially to promote the notion of trusted computer systems. As it's defined there these are computer systems which provide users with a high degree of confidence that the information that they have stored in those computers is protected from authorized—unauthorized use and disclosure. In short, computers that users can trust.

I was involved, prior to forming this company with—I was the director of information systems at the Office of the Deputy Under Secretary of Defense for Communications, Command, Control, and Intelligence. And among the things that I was heavily involved in was the development of computer security, techniques, and procedures during the last decade.

I spent 4 years at the Defense Advanced Research Projects Agency trying to promote the development of computer systems that you could trust; computer systems that were not vulnerable to some of the penetrations that we have seen that are available now with commercial products.

In 1978, I moved from DARPA over to the Pentagon and I established the Department of Defense computer security initiative. There were objectives for this. One was to coordinate the various computer research efforts going on then in the Department.

The second one, and this is probably the most important, was to encourage the development of trusted computer systems by the computer manufacturers themselves. I will talk more about that in a minute.

The third objective was to establish a process by which we could—we, the Defense Department—could evaluate computer systems and determine how vulnerable they were to penetration. Essentially the technologies had evolved sufficiently that we could quantify some number of levels of technical integrity and by that allow computers to be used in certain sensitive environments, whereas, they might not be useful in others.

I was very pleased that we were able to see the portion of the War Games movie that we did here. I would like to emphasize first that—as has not been implied here—that the national security aspects of that movie are nothing more than interesting fantasy. I have been involved both in NORAD system that was portrayed in the movie and in computers and it was in fact quite interesting to observe that the classified information on Defense Department computer systems is protected with physical and administrative procedural communications security techniques that are the best in the world.

There is no way that one from outside of that system can in fact gain access to those classified systems.

On the other hand, the things that we saw portrayed this morning with the young student gaining access to the school's computers and then programing his computer to go off and attempt to find all of the numbers on a particular exchange and then return within to a list of the ones that responded with a data tone. And then the intuitive process that he and his girl friend went through trying to find out that password—that magic password, was extremely well portrayed.

And I believe that every business individual who is—has any degree of sensitive information on his computer, really ought to see at least those portions. I wish we could have seen a little more of that part today, because they really do represent threats that are out there and that are quite real.

I believe that the notoriety of the 414's is not because they did anything new or unique, but really because they overdid it, and because they got caught. What they did requires, in fact, only a modest amount of equipment, access to a telephone, a little bit of knowledge but not really very much, in—about computers. And lots of young people in this country, and some not so young, I guess, have all of those ingredients. And I believe we are going to hear a good bit more about computer hackers in the coming months and years.

But the vulnerability we face is a lot more than just these hackers. We are moving into an area where, as has been discussed a number of times already today, our computer systems are being interconnected in very large networks going from the major financial giants to the local grocery stores. These provide incredible opportunities for fraud and for illegal manipulations, as Donn and others have talked about.

We need to worry about those highly sophisticated systems. We need to worry on one hand about the manager of one of those systems who says I don't really have a problem. I don't care, I am just going to go ahead and hook everything up. We need to worry—and, therefore, runs the risk of having his vital information in his company either destroyed or stolen, or whatever.

You also need to worry about the other side of this—the individual who gets overly frightened and says, well, I'll let all my routine and mundane stuff go on these computers, but I'm going to keep all my sensitive stuff off on an old manual system. You need to worry that part of it, too, because that, in fact, would cause a significant decline in the business effectiveness.

Management is probably the biggest problem in the computer security area—lack of awareness on the part of managers. Many of these happen because security is—doesn't contribute to the bottom line. It's—it's a deterrent from the uh—from the profit that makes a manager successful.

There are a lot of different aspects to the computer security problem. We've heard about many of the physical and administrative measures. We've heard about the notion that people will actually leave the active system account on a computer with the password that the manufacturer put in when he first started up. That's rather incredible and as Donn said, people who in fact do that, sort of deserve what they get.

These things are frequently overlooked by people who apparently don't seem to care about them. Many people have said that—that until users become aware and put into practice relatively simple and commonsense measures they have no need for the sophisticated trusted systems of the sort that have been coming out of the Defense Department research.

I agree, it's foolish for a computer containing sensitive information to operate a computer without such reasonable physical administrative measures. But the example of the 414's brings up a very significant problem. When a user who is remote from a computer can in fact, from thousands of miles away, gain access to that computer, it really doesn't matter if you have the best physical and administrative security measures or not.

Question of what we can do about the problem. The next topics that you asked for comment on deal with that. I spent 4 years at DARPA essentially trying to sponsor research at organizations like SRI and elsewhere to try to understand better how one could build a trusted computer system.

I became convinced in 1978 that the only way we were really going to make progress in this area other than by continuing to build research demonstration systems was to get the computer manufacturers involved in this process.

This is a major thrust of the DOD computer security initiative and one which I think is really showing some uh—some very high payoff. We have a number of the manufacturers that now are engaged in developing very high quality, high integrity trusted systems which will resist the uh—the attacks of hackers, whether they be malicious or not.

It's interesting the comments that were made at the end of the last talk about the economic effect of this—what are the things that are going to drive this? The insurance company's getting more involved in it.

We have a kind of a chicken and an egg problem. The manufacturers are saying, why should I get—bother with building better systems if nobody's out there demanding them? The—and the users, on the other hand, the banks and insurance companies are saying, not willing frequently to admit they have a problem because if they did admit they had a problem, they run the risk of their other competitors saying, gee, he's got a problem. I don't have that problem, you'd better move your stuff over to me.

Until they are certain that there is some solution that they can put into place, they are not going to—to admit that they have that kind of a problem. And so we go round circle with the manufacturers and say, well, no one's demanding it, why should I bother?

The Defense Department has been demanding these kind of things. There are major procurements now on the street in the Defense Department that are asking for high integrity computer systems. And we can see the beginnings of an impact of that on the computer manufacturers but the Defense Department is in fact quite a small segment of that process and so it's not going to have an effect—a very dramatic effect—early on.

We are seeing that, as I said, though, a way out of this maze. The computer manufacturers are beginning to work on systems like this; systems which will be much stronger in their ability to resist the kind of attacks that we are seeing on computer systems. And once those become commercially available in the next few years, I believe we are going to see a dramatic improvement in the overall situation.

Some of the concerns that you have expressed about why are we up against a situation where anybody can put anything into your computer and hide it there and you don't know anything about it. Well, these systems that we are talking about here have measures which isolate the security portions of the system and keep them from being able to be accessed from outside of the system. And these systems we will be able to say a great deal about whether or not they have been tampered with.

The existing systems where the security checks are scattered throughout the system, it is very easy to find ways to circumvent various of the controls. It is the purpose of these new systems that are being built now and will be available in the next 5 or 10 years to allow us to have a great deal of confidence that the kind of problem that you're concerned about, in fact, won't happen.

I have had quite a bit of experience in the question of what should the Federal Government do about these kinds of things. Summarizing my comments here, I was involved in the process of establishing the DOD Computer Security Evaluation Center where there was considerable discussion at various times during that process of whether that center should not be in fact a DOD resource but should be a Federal Government resource.

There was a period of time when we were exploring that actively where a Department of Defense organization and a Department of Commerce organization would jointly establish that.

At the time there was some resistance within the Defense Department to that and there was not a whole lot of interest on the part of the rest of the Government and so the Defense Department decided to go ahead with its own organization putting the center at the National Security Agency.

The reason for putting it there was that there was already in that location more computer security competence, a better technical structure on which to build such an organization.

But that brings up a problem because if we want to try to make this kind of information capability available to the rest of the Federal Government or to private sector, we are going to need a more open environment in which to do that.

And so I discuss in here several points about whether or not one should establish a Federal center. And NBS, of course, is a very logical place to try to do that. There aren't too many other choices.

But then we've got a problem of how to create the relationship between the DOD center and the NBS center. I don't come here with an answer to that. I do have some thoughts about it.

In the interest of time perhaps I will stop at this point and——

[The prepared statement of Mr. Walker follows:]

TRUSTED INFORMATION SYSTEMS, INC.
Computer Networking, Computer Security, Information Systems, Telecommunications

STEPHEN T. WALKER
PRESIDENT

September 26, 1983

Honorable Dan Glickman
Chairman
Subcommittee on Transportation, Aviation and Materials
House Committee on Science and Technology
United States House of Representatives
Suite 2321
Rayburn House Office Building
Washington D.C. 20510

Dear Chairman Glickman:

I appreciate the opportunity to appear before this Subcommittee on the subject of "Telecommunications Security and Privacy". My objective today is to point out the serious nature of the problems we face in this area, to describe some of the things which are underway now to deal with these problems and to discuss additional areas where work is needed in the near future.

Let me begin by describing who I am and why I believe this subject is particularly important at this time. I am President of Trusted Information Systems Inc., a small business which I recently founded. As the name implies, this business is concerned with development and use of computer systems which provide users with a high degree of confidence that their information stored in computers is protected from unauthorized use or disclosure; in short computers that users can "trust".

Prior to founding this company, I was the Director of Information Systems in the Office of the Deputy UnderSecretary of Defense for Communications, Command, Control and Intelligence at the Pentagon. In this capacity I was responsible for the World Wide Military Command and Control System (WWMCCS) Information System (WIS) and the Defense Communications System. I was also responsible for many of the advances in computer security within the Department of Defense (DoD) in the past decade. I spent four years at the Defense Advanced Research Projects Agency sponsoring computer security research activities. In 1978 I established the DoD Computer Security Initiative to 1) coordinate DoD computer security research activities, 2) encourage the development of

POST OFFICE BOX 45, GLENWOOD, MD 21738
301-854-6889 WALKER @ BBN

trusted computer systems by the computer manufacturers, and 3) establish a trusted computer system evaluation process to determine the quality of industry and government developed computer systems. In 1981, following extensive negotiations with officials in the DoD and various other government agencies, the DoD Computer Security Evaluation Center was established at the National Security Agency to carry on the efforts of the Computer Security Initiative.

With this as background, I am pleased to give you my opinions on the topics which you have posed for this hearing.

The first topic you asked to be discussed is: "current and future threats and vulnerabilities to our information/communication technology dependent society."

The highly popular movie "War Games" should be required viewing for all who are concerned with protecting sensitive information on computers. Let me state emphatically that the national security related aspects of the movie are nothing more than very interesting fantasy, similar to that portrayed in dozens of similar movies and books in recent years. U. S. Military data communications systems are protected with the best communications security mechanisms and procedures available in the world, and computers are always used in advisory roles with humans making all the essential decisions regarding use of military force.

However, this movie is much more than just another interesting tale of Armageddon because the measures that the young high school student takes to gain access to his school's computer, the phone number of the airline reservations service and the bank's computer are all very real and easy to perform using small personal computers. The idea of programming a computer to run through all the phone numbers in a given phone exchange and note the ones that return a "data" tone is neither new nor in the slightest way sophisticated. Once one has a target phone number, the intuitive process for guessing the password of a user (assuming the system even bothers with passwords) is very well portrayed in the movie. It is these more or less routine aspects of the movie that users of computer systems should concentrate on because they represent the potential serious threats that users face.

The notoriety that the "414s" group in Milwaukee received in the past few months is not because they did something new or unique, but because they overdid it, attempting to break into over 60 business and government computers, according to Newsweek, and they got caught. What they did requires a modest amount of computer equipment, access to a telephone, a little bit of knowledge about computers (but really very little to start with) and a lot of spare time. All of these ingredients are abundantly available to thousands of potential "computer hackers" today. We can expect to hear about many more "414s" in the coming months and years!

But our vulnerabilities in this field are not limited to hackers. The wide spread connection of major information processing facilities by communication networks is inevitable with our ever growing needs for rapid communication. This growth in all areas of the commercial and government marketplace, from the major financial institutions to the local grocery store, offers inviting targets, not just for computer hackers to experiment with, but for serious fraud and illegal manipulations. Many local systems that were reasonably protected as isolated computers become easy targets for exploitation when connected to a major network. As the hackers have shown, the technical capability to penetrate these systems exists. Some recent activities have indicated that the intent to do "malicious hacking" also exists.

We need these highly sophisticated automated capabilities to carry on the functions of business as we now know it. How many businesses could afford to operate without computers today? And we want ever expanding facilities to allow more rapid response, better control and other related capabilities. Some managers will proceed with rapid automation without consideration of the computer security vulnerabilities and thereby risk their company's future. Other managers, fearing the potential damage that malicious hackers might do, may decide to keep their most sensitive information off the advanced automated systems, restricting it to local, isolated processing systems. Such a development could have an equally damaging effect, resulting a serious loss in business effectiveness. Many of the most serious problems encountered in the computer security area are directly traced to lack of understanding by management. Even routine security measures are ignored because security does not contribute directly to the "bottom line" of profits.

There are many aspects to the computer and communications security problem. There are a significant number of routine physical and administrative measures that should be taken to protect information on computers as well as the computers themselves. If particularly important or sensitive information is on a computer, care should be taken to know who has access to the computer just as one restricts access to one's personal files. Many of these simple measures are overlooked by owners and users of computers either because they do not understand the vulnerabilities or because they don't care about them.

Many people say that until users become aware of and put into practice these relatively simple and common sense local practices, they will have no need for sophisticated trusted systems. While I agree that it is foolish to operate a computer containing sensitive information without reasonable physical and administrative security procedures, the example of the 414s points up the additional major problem which confronts us. Whether a system has good physical security measures or not doesn't really matter when an intruder using a phone thousands of miles away can guess a password, or tamper with the login security measures. Good physical and administrative procedures (including proper password controls) are important but no longer enough in themselves.

There is a growing tendency to use add-on security packages to attempt to enhance the integrity of existing systems. If these systems, with their limitations, are fully understood and carefully employed, they can contribute a degree of protection that is not available in present day commercial systems. Unfortunately as the extensive history of system penetration efforts over the past decade has shown, if these add-ons are blindly applied and relied on for full protection, they can be easily circumvented.

What can be done about this problem? Your next two topics deal with this issue: "the scope of telecommunications security research efforts; and the extent of Federal and private sector efforts in improving computer security". Following my four years of sponsoring research in trusted computer systems at DARPA, I was convinced that in order to make real progress, the computer manufacturers must get deeply involved. The steps needed to build a trusted system start with the very innermost functions of a computer operating system and its hardware support. Unless and until the computer manufacturers understand and begin to utilize and improve upon the technical solutions presently known, further government research would only produce additional testbed demonstration systems. Government funded research pointed out several viable approaches to building trusted systems; now we needed to leverage that research by reaching out to the development and engineering centers of the manufacturers to get them involved. This was the major focus of the DoD Computer Security Initiative from 1978 until 1981 and it has had considerable success. Several manufacturers now have significant efforts aimed at building high integrity trusted systems and more are getting involved daily. These systems are not easy to build, requiring several years to evolve into useful systems but once available they promise to provide facilities that are resistant to hackers, malicious or not.

With this shift of focus to the manufacturers for the basic operating system tools, the DoD research goals shifted to understanding applications of trusted computer systems for message handling and data base management systems for example. Other parts of the Federal government have conducted activities in computer security for many years. The Institute for Computer Science and Technology (ICST) at the National Bureau of Standards (NBS) has done a good job of quantifying the overall nature of computer security vulnerabilities and has promulgated standards such as the Data Encryption Standard (DES), a very useful capability for providing protection to computer communication systems. The Department of Energy has also done considerable work in this field in recent years.

Your fourth topic points up yet another interesting situation in this complex area: "the scope of related legal, social and economic factors affecting telecommunications security". Here we encounter another dilemma. The computer manufacturers claim that they cannot spend the extensive resources to develop trusted systems until there is a strong user demand. The DoD requirements are discounted because they represent only a small segment (5% or less) of the market and no manufacturer can develop a general purpose system for such a small market segment. The user community on the other hand, often ignorant of the vulnerabilities they face as well as the potential solutions, will not demand this capability until they are sure that the solution is in place. Any bank that admits it has a computer security vulnerability without having a solution immediately available, is inviting its customers to take their business elsewhere. Since the banks and other users will not admit to having a problem, we come back full circle to the manufacturers.

Fortunately there is a way out of this "chicken and egg" situation. As I mentioned several of the manufacturers have proceeded with efforts to develop trusted systems, anticipating the need. In the next few years as recognizably better systems become commercially available, the banks and insurance companies will be able to put in place a better system, offering "state of the art" protection to their customers and creating a rapidly growing requirement for such systems. Recent efforts by the Securities and Exchange Commission to require that companies give assurance to their stockholders that they are doing everything possible to protect the assets of the company will have a very positive impact on the marketplace for trusted computer systems once they become generally available.

Your final topic, "the appropriate role for Federal agencies" in this field, is a very difficult one. There are two major categories to be considered: the role within the Federal government itself and the role for the private sector. Within the Federal government there is much to be done. The DoD now has a reasonable capability; the CSEC will provide the center of excellence in the evaluation of industry and DoD computer systems. The results of these efforts will spill over into the rest of the government and the private sector as the generalized evaluation results of systems become known. But care must be exercised here! The DoD CSEC cannot and must not assume the role of giving advice to the other Departments of the Federal government. Situated as it is in the Intelligence Community such a role would be, I believe, most inappropriate. Prior to founding the Center at NSA, consideration was given to forming a Federal Computer Security Evaluation Center, located at NBS and jointly administered by the DoD and the Department of Commerce. However, considerable resistance to such a facility arose within the DoD and there was little support for the idea from other elements of the government. It was recognized at the time of the decision to locate the DoD center at NSA that this would have a limiting effect on the applicability of its results to the rest of the government. The value of locating the DoD center at NSA outweighed this potential future problem.

Some means must be found for offering direct support to the other major elements of the Federal government because the computer security aspects of the Social Security, IRS and similar activities are very serious. Establishment of a Federal Center, working closely with the DoD Center is a possibility and NBS remains one of the few logical choices for such a facility. But it will be essential (and very difficult) to ensure that the two organizations do not overlap, or worse, contradict each other. This will be a difficult situation to resolve.

As far as the Federal government's role for the private sector, I believe that the government should limit its efforts to a major education and awareness program concerning the computer security vulnerabilities and available solutions. Such an effort coupled with the evolution of market forces should be sufficient to advance the state of the art for at least the next few years.

I indicated when I began that 1. the problem was real, 2. considerable effort was already underway and 3. there are still many things to do. I would like to summarize some of the remaining actions in concluding my remarks. First and perhaps foremost is the need for the strong education and consciousness raising program that I just mentioned. Perhaps we should thank the "414s" for bringing this problem into general focus in a relatively benign way, though we must be careful not to dismiss the general problem as merely the work of some cranks. As people become aware of both the seriousness of the problem and the fact that solutions are possible, I believe the normal forces of the marketplace will cause corrections to come into place. But without a serious education effort, this process will take a long time. I believe that hearings such as these serve a very useful role in this context.

There are difficult problems in this area that can only be resolved successfully by the Congress. One of the more difficult ones effecting the private sector and non-national security portions of the Federal government is the problem of personnel security. How can one learn enough about the background of a person about to be entrusted with sensitive corporate information without violating that individual's privacy rights? The national security community has long had a classification system for labeling degrees of sensitive information and a clearance system for assessing the trustworthiness of its personnel. The rest of the government and the private sector have neither capability and as a result have serious difficulty resolving rather fundamental security protection mechanisms. This is a difficult problem for which Congressional resolution may be required.

As mentioned above there is a need for a capability to work directly with the major civilian government and private sector users of sensitive information systems. How such a capability can be established and its relationship with the DoD are difficult remaining questions.

There is a need for more research into all aspects of the computer security problem. There is a tendency to focus on the high technology issues and disregard the more mundane requirements such as improved physical and administrative measures. There is also a need to find the proper place for such research outside of the DoD and to provide consistent long term support for such activities.

I could go on at much greater length on some aspects of this very important field but I hope my remarks here will serve as at least a partial summary of where things are today and where we need to go from here. Again, I thank you for the opportunity to express my views.

Sincerely,

Steph T. Walk

Stephen T. Walker

Mr. GLICKMAN. Just quickly I want to ask you a question about national vulnerability and then move on to one generic issue because we need to leave the room in about 20 minutes. I want to give Mr. Nelson chances to ask questions.

You implied here that the war games scenario inasmuch as they relate to the entry into NORAD's computers were inaccurate and impossible.

Mr. WALKER. Yes.

Mr. GLICKMAN. Is that a fair statement?

Mr. WALKER. Yes.

Mr. GLICKMAN. Based upon your knowledge, do you believe that the classified and secure aspects of information in our Defense Department and related computers are safe from interference from either hackers or those with even more sinister motives?

Mr. WALKER. Classified information is protected. It is operated on in computers that are isolated in physically protected areas. And all of the communication links that link them together are protected with encryption capabilities so that the hacker problem getting on Telenet or the ARPANET or one of these other nets, they cannot gain access to those systems. Yes, that information is safe.

Mr. GLICKMAN. And you heard when Mr. Gore asked some of the questions about other ways to determine what's on a computer besides telephone lines, you know, some of the—were you here when he was talking a little bit—emanations——

Mr. WALKER. Oh, yes.

Mr. GLICKMAN [continuing]. And related things. And the New York Times had a story in yesterday's paper about other methods of getting into computers other than through telephone line. Is that part of your job you're—that you're working on now?

Mr. WALKER. Well, I'm certainly aware of the compromising emanations problem. And the same measures apply, the tempest measures apply to classified systems. They—all of the—you either have to put the computer in a physical room that itself is protected from emanations or the devices themselves have to be protected. The actual terminals that sit out in somebody's office have to in fact have a tempest certification so that somebody in the hallway or out in the parking lot can't pick up the information.

And these systems are protected against those measures also.

Mr. GLICKMAN. Let me ask you a question about the issue of national vulnerability raised by Mr. Parker before.

Let's assume for the moment that somebody—that the computer security system in our air traffic control operation was not as good as it should be and somebody could worm their way in there and change the location of blips on radar screens, or perhaps not quite as directly, but done—done so indirectly, that would obviously have catastrophic consequences on—on national vulnerability. And you could draw the same parallels with electric utility generating systems and railroad systems, all sorts of infrastructure issues. And you could do it also in the financial modal.

Mr. WALKER. Sure.

Mr. GLICKMAN. Are any of those scenarios possible?

Mr. WALKER. I am not familiar with the FAA—the FAA would be the most dramatic one. I am not familiar with that system but I don't believe that it's vulnerable to that. I believe that some of the—some of the things that the fellows did on the movie are done routinely.

Now, whether or not there are any banking systems that—that don't have sufficient protection against that or not, I—I doubt if all of them have sufficient protection that hackers who really wanted to get at them or malicious penetrators couldn't if they really tried.

Mr. GLICKMAN. Well, we'll—we're going to try to identify specifically what information people can get into in our later hearings because I think folks who have bank accounts or have credit cards ought to be assured that it is reasonably safe from this kind of operation, at least from the outside.

And I would ask you a final question with respect to the DOD Computer Security Center that you talk about in your testimony.

I wonder again if you would describe the purpose of that center, and is it fulfilling its purpose? Should it be expanded—maybe in—should communications security be added to this item?

Mr. WALKER. The center was formed in 1981 out of a corps of people at NSA. It has grown now very substantially and it has sufficient resources to grow. This is a difficult area to find experts. You don't find them just anywhere. And so you can't just instantly build a complete organization to do this.

I believe the center—the objective of the center is to promote the use of trusted computer systems; to promote the understanding of the computer security vulnerabilities and to find systems that are sufficient for use in particular environments.

It is heavily involved in the evaluation of DOD computer information systems. It is also involved, as I pointed out, working with the computer manufacturers. And it is my belief that that's the long-term answer to the problem, when we can get the average system that comes out of the manufacturer's—manufacturing plant. When the quality of that system can be substantially increased, that's when we are going to see widespread availability of these things.

Mr. GLICKMAN. Do you think that this center is fulfilling its purpose?

Mr. WALKER. I believe it is. It—one could hope that things would move faster but this is a very complex and difficult area. And the center is—is now firmly established. It has lots of—it has sufficient resources to do the job it has right now. And it is receiving considerable acclaim from folks that it's really taking on the job that it needs to do.

Now, the last part of that question was with respect to———

Mr. GLICKMAN. Should———

Mr. WALKER [continuing]. Communications security.

Mr. GLICKMAN. Yeah, should communications security be added.

Mr. WALKER. There is a whole large organization in NSA that deals just with the communications security problem. It's a separate organization because the problem there is frequently different. In dealing with encryption the Government essentially owns the encryption techniques and develops them themselves.

In dealing with the computer security problem, it's the manufacturers that own the system, not the Government. The Government———

Mr. **Glickman**. Some of the technologies may relate between the two.

Mr. **Walker**. Well, that's why it's useful to have the organization at NSA so that they can in fact share technologies. Unfortunately, the basic approach to the way you promote these systems is that it's different. And that's why they are—they are two separate entities.

But they are both under the same Director of NSA which allows him to make sure that things are melded together properly.

Mr. **Glickman**. Thank you.

Mr. Nelson.

Mr. **Nelson**. I have no questions, Mr. Chairman.

Mr. **Glickman**. We thank you very much for your testimony today.

This concludes the first day of these hearings. We meet the next time on October 17 and then a follow hearing—followup on the 24th of October to explore a variety of other issues relating to this subject.

This has been a fascinating hearing and I want to again thank all of the witnesses for appearing today.

[Whereupon, at 1:15 p.m., the subcommittee was adjourned.]

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

MONDAY, OCTOBER 17, 1983

House of Representatives,
Committee on Science and Technology,
Subcommittee on Transportation,
Aviation and Materials,
Washington, D.C.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2318, Rayburn House Office Building, Hon. Dan R. Glickman (chairman of the subcommittee) presiding.

Mr. Glickman. Good morning.

Today, the Subcommittee of Transportation, Aviation and Materials will resume its hearings on computer and communication security and privacy, a subject that was thrust into the news in recent months by a group of Milwaukee young people who succeeded in gaining unauthorized access to computers all over the country and, additionally, just late last week, the announcement of—that the FBI had seized the files and computer equipment in raids in cities including Detroit, Irvine, Calif.; Rochester, N.Y.; Tucson, and Oklahoma City in connection with a—an investigation which may involve a larger number of people.

Computers, of course, pervade our society. Few of us grasp fully the extent to which computers and the communications that link them affect our daily lives and the trend is toward ever greater use of this technology in the business world and in our homes in the future.

Yet, as our opening day of hearings on September 26 illustrated, there is a great potential for the misuse of computers and for unauthorized access to the data they contain.

Today we will turn to witnesses from the Federal sector. We will be examining the Government's need for security in its own use of computers and we will look at ways in which the Government can play a role with respect to the private sector's real need for security, such as sponsoring research, disseminating information, or perhaps passing laws.

The Government collects all kinds of information on its citizens: tax records, census, social security, law enforcement, and a whole assortment of other things and we want to make sure that this data is secure, that it cannot be in—improperly violated, either by outside persons or by the Government itself.

So these hearings ought to further examine the needs of what the problems are and what is available. I might also note for the record that recently it was announced that driven by increased concerns for computer security, the Defense Department yesterday, which was on October 3, ordered the separation of the Nation's oldest and largest computer network into civilian and military parts. The move is a key part in the Pentagon's 5-year plan to create its own defense data network, basically to protect the security of its system.

So obviously, this problem is one that involves both the civilian and military sectors of our Government and it's a pleasure to have a distinguished list of Government witnesses today.

Our first witness is the Honorable Joe Wright, Deputy Director, Office of Management and Budget, Washington, D.C.

Joe, it's a pleasure to have you here and why don't you come up.

Parenthetically, of course, we started our last hearing with clips from the movie "Wargames." I thought maybe we'd start with "The Right Stuff" today, but apparently other people have—have gotten that movie instead of us.

Mr. WRIGHT. It's early Monday morning—this is early Monday morning.

Mr. GLICKMAN. It's a pleasure to have you here.

Mr. WRIGHT. Glad to be here. I'd like to——

Mr. GLICKMAN. You may feel free to read your statement in its entirety or summarize it if you so desire.

STATEMENT OF JOSEPH R. WRIGHT, JR., DEPUTY DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET; ACCOMPANIED BY JOHN P. McNICHOLAS, CHIEF, INFORMATION POLICY, OFFICE OF MANAGEMENT AND BUDGET

Mr. WRIGHT. OK, thank you, sir.

With me is Mr. John McNicholas, who is the Chief of Information Policy at the Office of Information and Regulatory Affairs within the Office of Management and Budget.

I would just like to submit my testimony for the record if I may, Mr. Chairman, and just highlight a few points.

First, I want to start by saying, as you already know, the Federal Government is the Nation's largest user of automation—automated information. This year, we plan to spend about $12 billion on ADP and telecommunications equipment and by latest count, we've got between 18,000 and 19,000 medium- and large-scale computers at about 4,500 sites.

GSA estimates that by the end of the 1980's, this will get to be about 25,000 and, again, these are medium- to large-scale computers, and between 250,000 and 500,000 micros.

That will not be just an increase of 7,000 in terms of your medium- and large-scale computers, because my guess is that most of them will be replaced and so you're talking about awfully close to 25,000 in itself in terms of new computers of that type.

In the mid-seventies, congressional concern over a number of issues did help focus some attention and stimulated OMB's efforts in this entire area. Before that, computer security was really perceived to be the sole responsibility of the computer facility and the manager of that facility, rather than an overall management concern.

Again, because of many of the congressional oversight hearings and the concerns, OMB used the authority for ADP policy that was given to us by the Brooks Act and we did issue Transmittal Memorandum No. 1 to our circular A-71, which basically covered the requirements for Federal computer security programs.

We also at that time—at the end of the 1970's—required agencies to submit their plans for implementing the memorandum for OMB review, and a full review was done at that time. It has been updated through a series of processes, but we have not repeated that exercise because we feel at that stage we were able to go on ahead and focus enough attention from the agencies as to the needs for computer security.

However, things are changing dramatically right now as you know. The rapid growth and the reliance on information technology really brings to front the need for an effective Federal computer security program. We don't have enough coverage in the areas like microcomputers. We probably also don't have enough coverage in terms of the areas of telecommunications. Those areas were not a major concern during the mid-seventies.

But we believe that we've got most of the elements for a program of being able to put in the proper policy coverage and policy guidelines in place and I'll just cover those very briefly.

First of all, we are conducting our vulnerability assessments and internal control reviews under what we call our circular A-123 on internal controls. This was required of OMB as part of the Federal Managers' Financial Integrity Act and the first reports to the President and to the Congress from agency heads will be coming out the end of this year.

We have the President's Council on Integrity and Efficiency who has been working diligently to take a look at computer fraud and abuse. It came out with their first report recently and, of the 12 agencies responding, found a total of 172 cases. I think, Mr. Chairman, in looking at that report, I would say that I was surprised that the—incidences—number of incidences that were reported were so low, which would tell me one of two things: Either it is less of a problem than we thought—but my guess is that the reporting vehicles that we have are probably not appropriate, and we simply were not able to identify many of the cases. This is one of the areas we should focus on.

We also have the information resources management review process which fulfills OMB's responsibilities under the Paperwork Reduction Act. We also have OMB circular No. A-108, which is implementing the Privacy Act of 1974, in which agencies report to OMB how they intend to safeguard systems containing personal information prior to operating those systems. We review about 120 of those reports every year.

We also do a review of all matching program reports and have issued the guidelines to govern computer match operations, and then finally, Mr. Chairman, we have the budget review process which this year, for the first time, includes full management reviews of the agency programs, and one of the areas of management that we're specifically looking at is not only ADP plans from a hardware, software, and telecommunications point of view, but also from a computer security point of view.

Lastly, I would say that we are going through a fairly substantial exercise to be able to fill the gaps in policy and guidelines by updating the circulars on privacy and computer security. On September 12 of this year, we have invited public comment to rescind the existing information policy circulars and create a new one to bring them up to date which what we consider to be those needs within policy and guidelines.

We expect to have a full—first draft of this effort by the end of this year, and my best guess is we will probably coming out with a notice of proposed rulemaking sometime around spring or early summer, and then finally with the final—let's say mid next year sometime.

That concludes my formal statement, Mr. Chairman. I'd be happy to answer whatever questions you may have.

[The prepared statement of Mr. Wright follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

FOR RELEASE ON DELIVERY
Expected at 9:30 a.m.
Monday, October 17, 1983

STATEMENT OF JOSEPH R. WRIGHT, JR.
DEPUTY DIRECTOR
BEFORE THE SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIALS
OF THE COMMITTEE ON SCIENCE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES
ON OMB'S EFFORTS TO IMPROVE FEDERAL COMPUTER SECURITY

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss OMB's role in computer security. Recently, national attention has been brought to this topic by the real-life actions of the Milwaukee computer hackers as well as fictional exploits of the youthful protagonists of television shows and movies like *Wargames*. It is important to note that hackers represent but a tiny part of the problem. I commend your committee for holding these hearings and focusing public scrutiny on the broader aspects of this issue.

I believe the real significance of the *Wargames*/hacker phenomenon is not that a group of amateurs could break into important data bases, seemly at will. Indeed, the ease with which the so-called 414 group obtained access appears to be due more to the failure of management controls, i.e., laxness of the system operators in changing factory passwords, than to exceptional skill on the part of the group.

The real significance of this phenomenon is the extent to which we as a society are accepting and using computers in all facets of our lives without full recognition of their vulnerability. Sophisticated technology that a few years ago was the sole province of the technocrat is increasingly being placed in the hands of any user. Soon a computer in the home could well be as widely accepted as a telephone. Very basic changes are taking place in the ways in which our society operates; the automation of information processes is at the heart of these changes.

Naturally, the Federal Government has participated in this revolution since we are the nation's largest user of automated information. Our investment in information technology is huge: we currently spend about 1.6% of our budget for ADP and telecommunications equipment and services which, in 1984, represents over 12 billion dollars. The General Services Administration (GSA) estimates that we currently operate over 18,000 medium and large scale computers at some 4,500 sites. By the end of the decade that equipment total will grow to nearly 25,000. Moreover, as we integrate end-user computing into the management of our federal programs through the use of microcomputers, the GSA estimates we could have between 250,000 and 500,000 micros in place by 1990.

The Department of Commerce's Federal Information Processing Standards program is an effort to confront the very serious problems of hardware and software compatability that this exponential growth will bring. Uniform standards will enable agencies to share and consolidate information when appropriate.

If computer hackers pose a danger, it is that their activities may undermine the confidence of the public in our ability to protect the data that are essential to the operation of agency programs. Individuals may fear that others will be able to examine their tax records; corporations may fear that competitors will be able to uncover important information about their operations or manufacturing processes. And, fears like these may directly affect the quality of information our citizens furnish, thereby eroding the integrity of our data bases and ultimately affecting the quality of our programs.

In the mid 1970's, congressional concern over a number of issues helped focus our attention and stimulated our efforts in this area. Hearings leading to the Privacy Act of 1974 pinpointed the potential for harm that automated data banks might represent to individuals. In other hearings, the Congress focused on the operational integrity of important automated systems such as the NORAD Air Defense System and the FAA Air Traffic Control System. In addition, a 1976 congressional staff study focused directly on federal computer security and system integrity issues. As a result, OMB has been concerned about computer security for several years.

During the 1970's, computer security was perceived to be the sole responsibility of the computer facility rather than an overall management concern. To involve top management actively in this area, OMB used the authority for ADP policy given us by the Brooks Act (P.L. 89-306) and issued Transmittal Memorandum No. 1 to OMB Circular No. A-71. This circular, issued in July, 1978, established a basic federal computer security program. It requires that each agency head:

- Name a computer security officer for each computer installation;
- Establish personnel security policies which provide for screening of individuals involved in design or having access to sensitive computer processing systems or data;
- Establish a management control process to assure that appropriate levels of physical, technical and administrative safeguards are incorporated into data processing applications and facilities;
- Establish an agency program for periodic audits; and,
- Assign responsibility for the conduct of periodic risk analyses of each agency computer installation.

To broaden the base for oversight of this program OMB directed other central management agencies to provide assistance within their areas of expertise. Thus, Transmittal Memorandum No. 1 provided that the:

- Department of Commerce should develop and issue standards and guidelines for ensuring the security of automated information.
- GSA should:
  - -- issue regulations governing the physical security of computer rooms;
  - -- assure that agency procurement requests for computers or related services adequately incorporate computer security considerations;

-- assure that procurement specifications for computer hardware, software, facilities or services are consistent with Commerce, OMB and OPM standards; and,

- OPM should establish personnel security policies that provide for security consideration in the selection of personnel associated with design or operation of computer systems.

To ensure that each agency had an adequate computer security plan, OMB required agencies to submit their plans for implementing the memorandum for OMB review. In 1979, OMB assembled an interdisciplinary multi-agency team to review these plans and assess their strengths and weaknesses. All agencies were provided with critiques of their plans and were asked to revise them to overcome weaknesses revealed through the review process and to implement them.

These efforts represented the best available solutions for the time. But, we should remember that it was a time when most computer centers were discrete entities, telecommunications applications were limited, and agencies were not sharing much information. Our effort was aimed at putting some management controls in place quickly and we believe it resulted in the creation of a computer security program that was effective for its time.

OMB recognizes that times are changing dramatically. We have become substantially more dependent on automation for the operation of many federal programs. As federal programs grow larger, automation provides the most effective and efficient means of administering those programs. Manual systems in many cases are simply incapable of providing an acceptable alternative, even in the limited role of a backup system. The Social Security Administration processes 36 million retirement checks each month. Can anyone imagine doing all that by hand? Similarly, the Department of Defense operates the Standard Automated Material Management System which centrally manages the Defense Logistics Agency's two million stock items. This inventory is valued at approximately three billion dollars and annual issues of stock exceed 20 million separate items. Only in an automated environment could the Department meet its material management responsibilities with the speed and certainty national security requires. Computers now play a significant role in efforts to identify and bring waste, fraud, and abuse in government programs under control. Over the past six months, for example, use of computer matches in Food Stamp program investigations has resulted in 164 indictments of individuals for underreporting of income, according to the USDA Inspector General. Perhaps the most significant trend in automating federal programs is end-user computing in which program managers are responsible for their own processing rather than relying on a central ADP facility. It promises great savings through increased productivity, but it may exacerbate security problems.

This rapid growth in our reliance on information technology brings the need for an effective federal computer security program into sharp focus. We think that the elements of such a program are already in existence. OMB and the other central management agencies have produced a substantial body of material including directives, guidelines, and standards that deals with the problem of computer security. We are continuing to produce and update this material. If it were properly applied throughout the federal establishment, it would greatly enhance the security of our information systems.

In our view, the problem is that those tools often are not available to the managers who need them. There are two reasons for this: lack of information - the publicity/distribution process is inadequate; and lack of interest - managers often think about computer security only after the security of their systems has been breached.

In a recent study, which represents the most current data available on the extent of the computer security problem in the Federal Government, the President's Council on Integrity and Efficiency (PCIE) cited "lack of knowledge" on systems controls as a particular point of vulnerability. OMB is working to solve that "lack of knowledge" problem in ways I will describe shortly.

The lack of interest problem is harder to solve, but not impossible. In the national security and intelligence communities for example, computer/information security is an inseparable part of mission operations. A great deal of effort goes into ensuring security. All personnel are routinely and continually trained in security procedures. There are penalties for security violations ranging from administrative measures to criminal prosecution. The recent split up of the ARPANET system by the Department of Defense into two component parts, one containing operational information, the other scientific, indicates the seriousness with which that Department pursues the goal of computer security.

In domestic agencies, however, the consequences of computer system vulnerability are not as apparent to managers. As a result they often do not view security as an integral part of the operation of their programs. Since it has no visible payoff -- the end result of good security is that nothing changes -- there is a tendency to give this area low priority. We need to reach such managers and ensure that they are giving security proper consideration.

To this end OMB has a number of ongoing activities. Some are designed to gather information so that the Federal Government can determine the extent of the problem. Others are designed to ensure that managers are putting the proper management controls in place. Among these activities are the following:

- Vulnerability assessment and internal control reviews under OMB Circular No. A-123, "Internal Controls," and the Federal Managers Financial Integrity Act. The circular requires agencies to develop directives and plans for internal control systems to ensure the safeguarding of agency resources and assure the reliability and accuracy of its information. The Act requires reporting of the results to the President and the Congress. We expect that many agencies in performing vulnerability assessments and internal control reviews will follow the suggestion in the PCIE computer security report and give particular emphasis to assessments of the internal controls in automated systems.

- The efforts of the Inspectors General through the PCIE to define the scope of the computer security problem. While their initial effort represented the most extensive examination of computer fraud and abuse in federal systems to date, it was somewhat limited by the fact that agencies had not regularly tracked cases of computer fraud and abuse. Even so, the twelve agencies responding reported 172 cases (69 fraud and 103 abuse). Estimated losses ranged from $0 to $177,383 in fraud cases and $0 to $5,214 in abuse cases. The PCIE report recommended a continuation of this effort and OMB concurs in that recommendation.
- The Information Resources Management Review (IRM) process. These reviews flow out of OMB's responsibilities under the Paperwork Reduction Act to examine specific agency IRM activities. A number of these reviews focused on automated systems and computer security issues. For example, a study by the Department of the Interior showed that the department-wide effort to comply with the established directives on computer security was well below an acceptable level. The study recommended that a full-time departmental ADP Security Officer be appointed to manage the ADP Security Program. The Department is currently in the process of implementing the recommendations of the study in order to bring every bureau and office up to full compliance with security requirements.

- The Privacy Act system of records review process under OMB Circular No. A-108. This circular was aimed at implementing the Privacy Act of 1974 (5 USC 552a) and provided that each agency head should: "establish reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access and otherwise to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." The circular also requires that agencies report to OMB how they intend to safeguard systems containing personal information prior to operating those systems. OMB staff typically review 120 such reports each year. To date these reviews suggest agencies are appropriately matching the degree of protection needed with the sensitivity of the data in the systems.
- The review of "matching program" reports and the issuance of Guidelines to Govern Computer Match Operations. With the advent of computer matching of data bases containing personal information to further the government's anti-fraud and abuse efforts, OMB issued a set of Matching Guidelines. These were designed to insure that matching activities were conducted in conformance with the requirements of the Privacy Act and that matching agencies maintained effective security for the processes and the

data developed. This guidance was updated in 1982. The Matching Guidelines require matching agencies to submit reports on their activities to OMB and the Congress. Computer security is a key part of these reports. In addition, the Veterans Administration Inspector General developed for the PCIE a model control system for conducting matching programs which provides substantial guidance on computer security.

- The Budget Review Process. Through this process, OMB has helped agencies improve the security of many of their mission systems. For example, the Social Security Administration is presently engaged in a $500 million upgrade of its ADP systems and computer security considerations were a significant consideration in approving the resources for that upgrade. Likewise, the Internal Revenue Service is engaged in a computer upgrade budgeted at $214 million in FY 1984. Here too, computer security was a key concern.

In addition to these ongoing efforts, OMB is preparing to take some new steps. For example:

- We are in the process of updating our circulars on Privacy and Computer Security (A-108 and A-71). On September 12, 1983 we invited public comment on a proposal to rescind our existing information policy circulars and create a new circular that will address, in a comprehensive fashion, the entire spectrum of information resources management, including the safeguarding of automated information resources. We expect to have a first draft of this effort by the end of this year.

- We are working with Commerce's Institute for Computer Science and Technology (ICST) to help them better disseminate information about safeguards. ICST has tools that can help federal managers deal effectively with computer security problems. We are exploring methods for seeing that these tools are available to the managers. Among the possibilities are the development of training programs for top level managers and the operation of computer security conferences to highlight particular problems. Our aim is to bring the level of computer security awareness of the general federal manager to the same level as his military or intelligence counterpart.
- We are also exploring ways to tap private sector expertise in this area and to make that expertise available to the federal agencies. In areas such as electronic data funds transfers, we believe we have much to learn from the private sector.

In closing, let me reiterate that our interest in this subject is not a new one. It has been an area of concern to us for some time I can assure you, even when the publicity generated by the whizkids dies down, it is an area in which we will continue to be active.

This concludes my prepared remarks. I will be happy to answer any questions you may have.

Mr. GLICKMAN. Thank you, Mr. Wright.

Is it a fair statement to say that if there is any agency in Government responsible for coordinating the computer security communication security problem that it would be yours, the Office of Management and Budget?

Mr. WRIGHT. Yes, Mr. Chairman, that's a fair statement, but we also share those responsibilities with other central agencies, such as GSA, such as the Department of Commerce, National Bureau of Standards, and OPM.

I would also say that it's fair to put us in the role of primary oversight responsibility, but I would not want to take away from the fact that the—once we send out the guidelines and the policy, that the primary responsibility is the agencies themselves.

Mr. GLICKMAN. How large is your staff that you have at OMB working on the various activities you describe in your statement which are aimed at elevating the concern for computer security in domestic agencies?

Mr. WRIGHT. At ORA, that has the primary responsibility for this oversight, we've got a little over 50 people that are working on this directly. They are supplemented by—at budget time, our budget analyists, which we have about 190 that are working full-time with the agencies. We also, in the management reviews this year, will be bringing in around 110 combination of full-time and detailees working on it.

We also have the General Counsel's Office within our shop in which you've got 10, 12 people working on it. That's the OMB contingent.

Mr. GLICKMAN. OK. Have you noticed any—you talked about the fact that there were not a large number of reported problem areas. Have you noticed any particular agencies in which there are a higher number of reported problem areas in computer security?

For example, the Social Security Administration, perhaps. Banking, the FDIC, Comptroller, anything in particular that has caused you any degree of concern?

Mr. WRIGHT. John, maybe you'd know that. Of the report they came up with, which of the agencies they had the highest number of incidents?

Mr. MCNICHOLAS. I don't have the report in front of me here, but I believe that we find that the largest incidents of possible problems occur in those agencies that have major financial operations.

Mr. GLICKMAN. Major financial?

Mr. MCNICHOLAS. Major financial operations, such as the Social Security Administration.

Mr. GLICKMAN. This report—is this—when was this report completed and is this something the committee has access to?

Mr. WRIGHT. Yes, sir, Mr. Chairman, we'll be more than happy to get you a copy if you don't already have it. This was done this year.

Mr. GLICKMAN. OK. But—again, the report doesn't show anything particularly unique or overwhelming in terms of the number of problems in any of the agencies?

Mr. WRIGHT. It has—I guess if you have to say what is one of the overriding recommendations they come up with--and I mention this in my testimony—was the lack of information that is provided to the managers within these agencies of exactly what the policies and the guidelines are and they also, I believe, referred to a lack sometimes of the proper amount of attention that's paid to computer security.

Mr. GLICKMAN. I see here on page 7 of your statement, the report cited lack of knowledge on systems controls as a particular point of vulnerability and again you indicate that at this stage, you are not absolutely sure—you have no scientific evidence that the number of reported problems may, in fact, be less than what is actually occurring because of the inability to obtain that information.

Mr. WRIGHT. Yes, sir, that's right. Also, we don't have a good data base in this area. This is something that I believe that the Federal Government should start developing. If nothing else, to be able to provide good guidelines across agency lines as to the problems that are occurring and the solutions and the safeguards that have to be put in place.

Mr. GLICKMAN. Is the problem that you have identifying what is a computer crime?

Mr. WRIGHT. I don't believe we have a problem on identifying what is a computer crime so much, although some of these headlines in recent—you know, tend to take on a little bit of the—kind of the spirit of adventurism and all of the rest of it and I don't believe they properly define exactly what is a crime as well as we'd like to see.

If you just access into a data base and you don't have proper authority to access that data base, is that a computer crime, and I believe that some clarification could be used there, particularly with—which you have a lot of these kids; they weren't necessarily doing anything with it; they were just accessing. And I believe—if whether we have to define computer bases in some way or another, I think we ought to identify that as a crime.

Mr. GLICKMAN. Because the mere accessing to certain records—let's say Social Security——

Mr. WRIGHT. Sure.

Mr. GLICKMAN [continuing]. Is a violation of probably some of the existing privacy statutes, even if nothing is changed within that.

Mr. WRIGHT. Even if nothing is changed, and I believe some clarification would be very helpful there.

Mr. GLICKMAN. Now, you're talking about clarification from Congress in terms of the law or——

Mr. WRIGHT. Clarification from Congress; yes, sir. There's not much that we can do from the executive branch except for establish what the policies and the guidelines are. It's very, very difficult for us to get beyond that except in those areas that you're mentioning on the invasion of privacy area as to where we can then go in and put in the—but, for example, I believe unless it's clarified, that you will have a situation to where you can have somebody access a data base, change that data base like, perhaps, like they did in this one hospital case that I've heard about, and may not even be meaning to.

Mr. GLICKMAN. May not be--I'm sorry, I didn't hear you.

Mr. WRIGHT. That may not be their intent.

Mr. GLICKMAN. Yeah.

Mr. WRIGHT. And so, you know, I've got some very serious questions in that area.

Mr. GLICKMAN. On page—you've kind of touched on this. On page 5 of your statement, you mention review of agency computer security plans to judge their adequacy.

Mr. WRIGHT. Yes.

Mr. GLICKMAN. What criteria did you use and how were they developed?

Mr. WRIGHT. OK, Mr. Chairman. What we did was at that time, we developed a list of criteria as to what we thought were the requirements for effective computer security programs along with other central agencies such as GSA, and then we used those criteria in order to evaluate the plans.

We'd be more than happy to submit those.

Mr. GLICKMAN. If you would, I'd appreciate it. That would be useful for the hearings.

[The information follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEC 1 1983

Honorable Dan Glickman
Chairman, Subcommittee on
Transportation, Aviation and Materials
Committee on Science and Technology
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This is in response to your letter of October 20, 1983 to the Director of OMB which asks for supplemental information concerning my testimony of October 17th.

In response, I am enclosing the following:

- o An edited transcript of my testimony;
- o Supplemental materials I agreed to supply during the hearing;
- o Responses to the questions you submitted subsequently.

I look forward to reading the Committee report.

Sincerely,

Joseph R. Wright, Jr.
Deputy Director

Enclosures

January 1979

AGENCY COMPUTER SECURITY PROGRAM CHECKLIST

Use: To determine whether agency security programs conform to the requirements of OMB Circular No. A-71, Transmittal Memorandum No. 1 dated July 27, 1978.

Agency:____.

Date of Plan(s):____.

ASSIGNMENT OF RESPONSIBILITY FOR COMPUTER SECURITY

( ) Has the agency identified the individual having lead responsibility for computer security?

- ° Name of Individual______________________________.
- ° Title____.
- ° Mailing Address__________________________________.
- ° Phone Number____________________________________.

( ) Has the agency assigned responsibility for computer security at each headquarters and field organization?

( ) Have the names and titles of individuals responsible for computer security at each facility/installation been identified?

( ) Do the individuals assigned responsibility for computer security have both computer and security experience?

( ) Has responsibility for computer security been formally assigned?

- ° By delegation memo?______________________________
- ° By job description?______________________________
- ° By charter statement?____________________________
- ° Other?____

MANAGEMENT CONTROL PROCESS FOR COMPUTER APPLICATIONS

( ) Has the agency described a management control process to assure that appropriate administrative, physical and technical safeguards are built into all computer systems?

( ) Has the management control process been formally promulgated?

( ) Does the process allow for evaluation of the sensitivity of each current and new computer application?

- ° Does the process define the relative roles of the user, developer and operator of systems in determining the sensitivity of systems?

- ° Who makes the final system sensitivity determination?

SECURITY SPECIFICATIONS

( ) Does the agency management control process provide for defining and approving security specifications prior to programming new applications or making significant changes to old applications?

( ) Does the security specification development and approval process provide for consideration of the views of the user, the developer, the service organization, the individual assigned responsibility for computer security, and agency audit staff?

( ) Does the process define "significant changes to existing systems" and establish procedures for approval of security provisions prior to making changes to existing systems?

( ) Does the plan identify a date by when a review of security specifications for existing systems will be completed? Dates by when corrective action will be completed?

( ) Is the final authority for approving computer system security specifications clearly defined and formally established?

- ° Who makes the decision?___________________________

( ) Do the procedures assure that provisions of the approved security specifications are incorporated in agency administrative procedures and programming specifications?

- ° Who is responsible for follow-up?________________

DESIGN REVIEW PROCESS

☐ Do the agency procedures establish requirements and responsibilities for conducting design reviews?

☐ Does the design review process provide checks and balances to assure adherence to the approved security specification?

☐ Does the procedure provide for documenting design review results?

☐ Is the responsibility for approving system designs subsequent to design reviews established?

- Who approves?________________________________

SYSTEM TEST PROCESS

☐ Do the agency procedures establish requirements and responsibilities for conducting and approving systems tests?

☐ Are the relationships between the design review process and system test processes established?

☐ Do the agency's system test procedures require testing of all aspects of security -- including administrative procedures, financial checks and balances, physical security and technological security features?

☐ Are the results of previous audits considered in the test procedures?

☐ Does the procedure provide for documenting system test results?

☐ Are responsibilities for conducting system tests established?

- Who is responsible?___________________________

SYSTEM CERTIFICATION PROCESS

☐ Does the agency management control process preclude operation of any new or modified system prior to satisfactory completion of systems tests?

( ) Do the certification procedures assure conformance to approved security specifications?

( ) Do the certification procedures assure that all applicable Federal policies, regulations, and standards have been complied with?

( ) Do the procedures provide for periodic recertification of systems?

( ) Do the procedures provide for certification of all current operational systems?

° When will they be completed?

( ) Does the agency program define policies, criteria, and timetables for periodic recertification of systems?

( ) Are responsibilities for certification and recertification of systems established?

° Who is responsible?________________________________

AUDIT/EVALUATION REQUIREMENTS

( ) Does the agency programs make a distinction between security audits and security evaluations?

( ) Have audit requirements been formally established?

° Who is responsible?__________________________________

( ) Have evaluation requirements been formally established?

° Who is responsible for the evaluation program?

° What organizations will participate in the security evaluation process?

( ) If agency program includes both audits and evaluations -- has a coordination mechanism been established between audit and evaluation groups?

° Who is responsible?________________________________.

( ) Has a master audit/evaluation schedule been prepared?

° Have criteria been established for determining the priority of audits/evaluations?

  - Are high risk or highly sensitive applications identified?
  - Have timetables been established for conducting audits/evaluations of all sensitive applications established?
  - Is the interval for periodic audits/evaluations equal or less than three years?

( ) Is the audit or evaluation performed by an organization independent of the user and computer facility manager?

( ) Have computer audit and/or evaluation guidelines been established?

( ) Where applicable, are computer system audit requirements included in agency IG implementation plans?

( ) Are the documented system security specifications, design review results, system test results, and system certifications made available to the audit and evaluation staffs?

( ) Has the agency established an information system audit/evaluation training program?

( ) Does the audit/evaluation function include

  - Examination of data sensitivity?
  - Verification and validation of the adequacy of physical, administrative, financial, and technical control?
  - Adequacy of security administration?

RISK ANALYSIS PROCESS

( ) Has the agency assigned responsibility for conducting periodic risk analyses?

  - Who is responsible?______________________________.

( ) Does the risk analysis adequately measure the vulnerabilities at the installation?

  - Related to the potential for fraud or theft?

- ° Related to the potential for inadvertant error or improper disclosure of information?
- ° Related to the potential financial risk?
- ° Related to the potential of causing harm to individuals or infringing on their rights of privacy?
- ° Related to the protection of proprietary data and potential harm to business?

( ) Has the relationship between the organization responsible for conducting risk analyses and other organizational elements been defined?

- ° Relationship to IG function?
- ° Relationship to audit function?
- ° Relationship to evaluation function?
- ° Relationship to inspections function?
- ° Relationship to security function?
- ° Relationship to program office?
- ° Relationship to computer operational function?

( ) Are requirements established for the conduct of risk analyses for government-owned-contractor-operated (GOCO) facilities as well as government operated facilities?

( ) Does the agency program include provisions for assessing risks related to computer services provided by other agencies and those provided through commercial services?

( ) GSA only - Have provisions been made to assess risks of government-wide services provided to agencies by or through GSA, to advise agencies of the level of security provided by those services?

( ) Where applicable, are the requirements for computer risk analyses included in agency vulnerability assessment plans being developed to implement the I.G. legislation?

( ) Has a specific timetable for conducting risk analyses been established?

- ° Is the interval between risk analyses commensurate with the sensitivity of the information processed?
- ° Is the interval between risk analyses less than five years?

( ) Where sensitive applications represent only a small portion of the workload of a particular computer, has consideration been given to moving the applications to a secure installation and avoiding the need to secure the complete installation for a small portion of its workload?

( ) Do the agency procedures require that a risk analysis be performed:

- ° Prior to the approval of design specifications for computer installations?
- ° Whenever there is a "significant change" to the physical facility, hardware or operating system software?

( ) Has the agency defined "significant change"?

( ) Is the definition of "significant change" commensurate with the sensitivity of the information processed by the installation?

( ) Are NBS draft guidelines on conducting risk assessments included in agency guidance?

PROCUREMENT REQUIREMENTS

( ) Have agency policies and procedures been established to assure that security requirements are included in specifications for:

- ° Equipment?
- ° Computer processing services?
- ° Facility management services?
- ° General purpose software?

- ° Operating system software?
- ° Design or programming of applications?

( ) Are the specifications reviewed by the security official to verify that:

- ° They are reasonably sufficient for the intended application.
- ° That they comply with current Federal computer security policies, procedures, standards and guidelines.

( ) Have the requirements been incorporated in the agency procurement policies and regulations?

( ) Do the procedures require review of the adequacy and security provisions in current contracts, consider the feasibility of renegotiating existing contracts where appropriate, or modifying the terms of existing contracts prior to renewing the contracts or exercising any extension options under the contracts?

( ) Has responsibility for these matters been assigned?

- ° To whom?____

CONTINGENCY PLANS

( ) Has the agency established policies and responsibilities to assure that contingency plans (in the event of natural disaster, hardware/software failure, or any events which could cause a significant description of service) are developed and maintained?

( ) Are the contingency and back-up requirements established by the agency commensurate with the risk and magnitude of potential loss?

( ) Are the contingency plans reviewed and tested at periodic intervals? What intervals?_____________________________

( ) Are the test intervals commensurate with the risk and magnitude of potential loss?

PERSONNEL SCREENING REQUIREMENTS

( ) Has the agency established personnel security policies for screening individuals?

( ) Does the personnel policy provide for levels of screening commensurate with the sensitivity of the function?

( ) Do the agency policies and criteria consider separation of duties in sensitive processes so that each position would be less sensitive?

( ) Have screening requirements for contractor personnel been established and implemented?

( ) Are the personnel policies consistent with FPM letter 732-7?

RESOURCE ESTIMATES ($ in thousands)

One-time Costs. Staff-Years__________$_____________

On-going Costs. Staff-Years__________$_____________

GENERAL COMMENTS

REVIEWER:____________________

DATE:________________________

COMPUTER-RELATED FRAUD AND ABUSE IN GOVERNMENT AGENCIES

Richard P. Kusserow
Inspector General
U.S. Department of Health and
Human Services
June 1983

EXECUTIVE SUMMARY

The President's Council on Integrity and Efficiency (PCIE), because of its concern over the need for increased computer auditing and computer security expertise within the Inspector General (IG) community, directed the IG of the Department of Health and Human Services (HHS) to provide the Council with a perspective on the nature and scope of computer-related fraud and abuse in Government agencies. To accomplish this, the HHS-IG convened an interagency task force to survey the agencies about the known instances of computer-related fraud and abuse. The survey requested information on cases discovered between January 1, 1978 and March 31, 1982, and yielded the following:

Findings

- Scope of Response - The extent of computer-related fraud and abuse known to Government agencies cannot be determined because agencies did not systematically track these cases. Despite this constraint, 12 agencies did respond with a total of 172 cases (69 fraud and 103 abuse) which met the survey criteria.
- Nature of the Cases - Fraud cases primarily involved theft of cash or diversion of assets, usually in benefit funds disbursement or payroll systems. Most frauds involved input techniques, such as the introduction of false transactions or records. The majority of abuse cases, however, involved theft of computer time through creation or use of programs for personal/outside business or entertainment.
- Perpetrator Characteristics - Three-fourths of the cases involved only one perpetrator, who was usually a Federal, nonsupervisory employee. Perpetrator characteristics, however, differed for fraud and abuse cases in the following ways:
  - -- Four out of five of the fraud perpetrators earned $20,000/year or less, but almost half of the abuse perpetrators earned over $20,000/year.
  - -- Two-thirds of the fraud perpetrators were functional users of the system while three-fifths of the abuse perpetrators were data processing personnel.

- Loss - Loss estimates in fraud cases ranged from $0 to $177,383, although almost half of the respondents stated that they felt actual losses were higher. Abuse cases had very scant (33%) response on loss estimates, with responses ranging from $0 to $5,214.

- How Detection Was Triggered - In both fraud and abuse, half of the cases were detected by accident, which was twice the incidence of detection through controls. Controls, however, were responsible for a higher proportion of detection in payroll systems (46%) than in benefit systems (12%).

- Who Detected Cases - Agency personnel found over half of the frauds and over two-thirds of the abuses. Within agency personnel, co-workers found twice as many abuses as managers.

- Response on Systems Controls - Although the survey asked specific questions regarding the state of controls in victimized systems, one-fifth of the respondents did not answer at all, and many others gave incomplete or illogical responses. A high proportion of respondents were unable to answer whether the victimized system had been audited or reviewed, nor did they know whether formal risk assessment programs were in place.

Conclusions and Recommendations

- Further Survey Work - While the data do provide a picture of the reported instances of computer-related fraud and abuse, more work needs to be done to assess the limits of the survey data and build upon it as an ongoing source of information and analyses. Therefore, we recommend that:

  - The Task Force conduct Phase II of the study to determine the causes of data limitations, the extent of computer security awareness in IG organizations, and the state of controls in victimized systems.

  - The PCIE should maintain this unique data base by conducting periodic survey updates.

- Training and Awareness - The incomplete responses on systems controls and prior audits implies a lack of knowledge of these areas by respondents, who were primarily investigators. To improve awareness and expertise, the Task Force recommends that:

-- IGs provide training to investigators on the internal controls of automated systems.

-- Investigators be made aware of the documented vulnerabilities in their agencies' automated systems.

o Controls in Automated Systems - The high proportion of cases detected by accident is alarming because of the implication of weaknesses in internal controls and the potential for undetected fraud and abuse. Since OMB Circular A-123, which is now being implemented, provides a framework for identification and correction of internal control vulnerabilities, the Task Force recommends that:

-- Agencies give particular emphasis in their A-123 internal control reviews to assessments of the internal controls in automated systems.

-- The PCIE establish a system to alert IGs to generic computer system control weaknesses to enable IGs to focus on common prevention strategies.

ACKNOWLEDGEMENTS

This report is the product of many efforts over long months. I have been fortunate to chair an interdisciplinary Task Force of experts from the various Office of Inspectors General and related organizations. Their keen interest in the subject and generous contributions have made the process of this survey, as well as the product, a valuable asset to the IG community. Although many staff have been involved during the course of this study, I would especially like to thank Sheila Brand, Department of Defense; Robert McKenzie, National Aeronautics and Space Administration; John Newell, Department of Commerce; Robert Ryan, Department of Defense; Warren Seitz, Department of Agriculture; Mike Sielicki, Department of Treasury; Dale Stewart, Department of Commerce; James Watts, General Accounting Office; and, from my staff, Jane Tebbutt, project manager, and Gail Shelton. Dr. C. Mitchell Dayton, University of Maryland, provided extensive and professional statistical consultation and computer services. Finally, I wish to note the services of the HHS Planning and Evaluation Graphics staff for providing the tables and Bertha Hunt for tireless and unfailing typing support.

Richard P. Kusserow

Richard P. Kusserow
Inspector General
Department of Health and
Human Services

INTRODUCTION

The U.S. Government owns or operates more than 16,000 computer systems. The applications run on these systems range over such diverse areas as national security, scientific or economic data, benefit payments, and payroll. Without the computer, most of these functions could not be accomplished.

Yet, our almost total dependence on computer systems causes continuing problems for the Government manager. Computer systems process enormous volumes of data with little human intervention, resulting in the concentration of the remaining manual functions into fewer hands, with little separation of duties. Rapid computer technological advances create a dependence on a relatively small number of data processing technical experts. Just as important, the computer itself represents a valuable resource to be protected from accidental or intentional loss of availability.

The vulnerabilities of computer systems to fraud and abuse have been reported for a number of years:

- In 1977, a staff study of the Senate Committee on Government Operations cited that "...the Federal Government has taken appropriate steps to insure the integrity of those computer systems which process national security data...But there are no corresponding safeguards, standards or adequate security procedures in many Federal programs unrelated to national defense."[1]

- The former Law Enforcement Assistance Administration's manual on computer crime states that "Unfortunately, ...businesses, government agencies, and institutions that use computers for technical and business purposes... (are) neither adequately prepared to deal with nor sufficiently motivated to report this new type of crime to the authorities."[2]

- The U.S. General Accounting Office reviewed Federal systems and found that "...executive agencies' automated information systems and the assets they control are exceedingly vulnerable to misuse, abuse and theft."[3]

In the 95th Congress (S. 1766), and again in the 96th (S. 240) and 97th (H.R. 3970), Federal legislation has been proposed which would make computer fraud a Federal offense. On January 31, 1983, Congressman Bill Nelson reintroduced the Federal Computer Systems Protection Act (H.R. 1092). Amidst the debate regarding the need for and provisions of such legislation, several points of consensus seem to emerge:

- Computer fraud and abuse do exist. Perceptions about the size of the problem, however, vary widely.

- No data exist which define the scope of the problem either in Government or the private sector, although case histories gathered by experts describe a variety of computer-related incidents.

- While no computer system can ever be entirely secure, most systems, particularly those with non-defense related applications, lack sufficient controls to afford an adequate level of protection from computer-related fraud and abuse.

The President's Council on Integrity and Efficiency (PCIE), because of its concern over the need for increased computer auditing and computer security expertise and activity within the Inspector General (IG) community, directed the IG of the Department of Health and Human Services to lead a computer security project for the Council. The task force he convened includes experts in computer security and computer auditing from the Departments of Agriculture, Commerce, Defense and Treasury; the National Aeronautics and Space Administration; and the General Accounting Office.

OBJECTIVE OF THE STUDY

The PCIE charged the task force to provide the Council with a perspective on the nature and scope of computer-related fraud and abuse in Government programs. Specifically, study objectives were to answer the following questions about computer-related fraud and abuse:

- Is there a problem?
- If so, what are the characteristics?
- What should the Inspector General community do to detect/ prevent future instances?
- What additional computer security expertise and activity are required in the IG environment?

SCOPE AND METHODOLOGY

To accomplish this objective, the task force undertook a survey of the known computer-related fraud and abuse cases in Government agencies. Although a few other reports of computer-related crime have been published (notably a 1976 study by the General Accounting Office[4]), this PCIE study is the first systematic data collection effort of its kind in the Government.

The study involves a two-phase approach: a survey phase and a followup interview phase. This report presents the findings of Phase I.

The task force decided to include both fraud and abuse in the scope in order to obtain the broadest possible data base and to ascertain the similarities and differences in the two subsets. For this purpose, the following definitions were developed:

> Computer-related fraud is any illegal intentional act or series of acts that is designed to deceive or misrepresent in order to obtain something of value. Further, a computer system must have been involved in the perpetration or cover-up of the act, or series of acts. A computer system might have been involved through improper manipulation of: (1) input or transaction data, (2) output or results, (3) applications programs, (4) data files, (5) computer operations, (6) communications, or (7) computer hardware, systems software, or firmware.
>
> Computer-related abuse is the misuse, destruction, alteration or disruption of data processing resources. The key aspects of computer-related abuse are that it is intentional and improper, but it does not necessarily imply the violation of a specific law nor the presence of false representation. Examples of computer-related abuse are (a) unauthorized use of the computer by Federal employees for their personal programming activities, and (b) misuse of computer equipment for revenge against a government agency.

These definitions served both as instructions to respondents and as criteria for later analysis. In the case-by-case analysis stage, the definitions were further refined, specifically in the cases involving theft of computer time. The task force recognized that computer time is often considered an asset and that the unauthorized use of the computer can be discussed in terms of fraud. For analysis purposes, however, the task force, after lengthy debate, decided to classify this type of case as abuse.

To survey the agencies regarding their known cases of computer-related fraud and abuse, the task force developed a questionnaire (Appendix A) patterned after a survey instrument designed by the American Institute of Certified Public Accountants (AICPA) for their as yet unpublished study of computer fraud in the banking and insurance industries.

The questionnaire instructed respondents to complete one survey form for each case of computer-related fraud and abuse discovered between January 1, 1978 and March 31, 1982. (The beginning date was chosen to coincide with the advent of most IG organizations.) The questionnaire requested information in the following areas: (1) type of computer-related fraud or abuse, (2) perpetrator profiles (for up to four perpetrators per case), (3) case description, (4) detection method, (5) computer environment, (6) methods of perpetration and concealment, and (7) effectiveness of controls and audit procedures.

The survey forms were directed to the Inspectors General and other members of the PCIE, plus the Federal Bureau of Investigation (FBI), U.S. Secret Service, and the Chief Postal Inspector. Upon receipt of the completed survey forms, the task force reviewed the cases for completeness and eliminated those cases from the total which did not meet the definitions of computer-related fraud and abuse. Cases were then given a preliminary analysis to categorize and prepare them for computerized statistical analysis.

FINDINGS

The degree to which cases are in fact detected and/or reported cannot be estimated. Although originally charged to discover the scope of computer-related fraud and abuse in Government programs, the task force rapidly became aware that this was not possible. As noted in a 1976 GAO report, agencies do not differentiate between computer-related and other types of white collar crimes.[4] Instead, the task force had to rely on individual memory and/or *ad hoc* information systems which agencies may have instituted. To add to these constraints, neither the FBI nor Secret Service was able to respond to the survey because their case files are all kept in their field offices and would require a prohibitive amount of time to research.

Such problems should decrease in the future, at least for criminal cases. As a result of our survey and their concern for the problem, the Justice Department's newly implemented Fraud and Corruption Tracking System (FACTS) will uniquely identify all computer-assisted fraud cases referred to the FBI and/or the U.S. Attorneys. In response to our inquiry, the U.S. Secret Service has also stated that its information system will now identify computer-related fraud cases.

What Was the Response to the Survey?

The following agencies reported cases to the task force:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Justice
Department of Labor
Department of State
Department of the Treasury
National Aeronautics and Space Administration
Office of Personnel Management
Veterans Administration

Within these agencies, the majority of individual respondents represented the investigative community (70%), composed of both IG investigators (20%) and internal agency investigators (43%) or security officers (7%). The other respondents represented program/functional personnel (7%), data processing personnel (4%) and unspecified job types (18%).

Of the 215 responses to the survey, 43 were eliminated since they did not meet the definitions of computer-related fraud or abuse. The remaining 172 cases comprised 69 fraud and 103 abuse cases.

The fraud cases primarily (93%) involved theft of cash or diversion of other assets, and over three-fourths of these cases entailed a fictitious or unauthorized benefit (59%) claim or an unauthorized payroll payment (21%). Abuse cases primarily involved theft of computer time (57%), theft of data (13%) and/or destruction or alteration of data (17%).

The majority of both fraud and abuse cases involved in-house (agency operated) facilities (80%) and occurred during normal processing (89%). The systems involved employed a variety of different types of computer technology: 48 percent involved batch processing; 41 percent involved on-line, real-time processing; 33 percent involved on-line inquiry capabilities; 28 percent involved centralized processing; 22 percent involved remote batch; and or 16 percent involved data base management systems (percentages total more than 100% because of multiple answers).

Who Were the Perpetrators of Computer-Related Fraud and Abuse?

Seventy-five percent of the total cases involved only one perpetrator (referred to below as the primary perpetrator). This proportion was somewhat lower for fraud (65%) than for abuse (82%) cases, indicating that collusion either is more common in fraud cases or is at least more investigated or documented.

The survey data provide the following profile of the primary perpetrators of computer-related fraud and abuse:

TABLE 1
Characteristics of the Primary Perpetrators

Characteristics	Percentage of Primary Perpetrators[5]	
	Fraud	Abuse
Employer:		
- U.S. Government	66	79
- State/local	22	1
- Private Sector	12	20
Level of Employee:		
- Nonsupervisory	77	73
- Supervisory	23	27
Annual Salary:		
- $20,000 or less	81	51
- $20,001 - $50,000	19	43
- Over $50,000	0	6
Job Area in Relation to the Computer:		
- Functional User	62	30
- Data Processing Personnel	30	59
- Other (outsiders, unknown job types)	8	11
Disciplinary/Legal Action Received after Detection:		
- No Action	16	30
- Judicial Action (with or without administrative action)	74	9
- Administrative action only	10	61

As shown in Table 1, the most noticeable differences between the primary perpetrators of fraud and abuse are in the areas of salary, job area, and disciplinary or legal action taken:

- While four out of five of the fraud perpetrators earn $20,000 or less, almost half of the abuse perpetrators earn over $20,000.
- Almost two-thirds of the fraud perpetrators are functional users of the system, but almost three-fifths of the abuse perpetrators are data processing personnel.
- Although three-fourths of the fraud perpetrators were subjects of judicial action, only about one in ten abuse perpetrators were subjects of any judicial action.

Since the nature of abuse is characterized by a high proportion of use of computer resources, the higher proportion of data processing personnel, who have access to and knowledge of programming and operations, may be expected. The low proportion of data processing personnel in fraud cases may be understood more fully after presentation in the next section of the techniques employed to perpetrate the fraud or abuse.

The difference between fraud and abuse in salary may be understood in terms of motive. In 93 percent of the fraud cases, the motive was financial gain, as opposed to 6 percent in abuse cases. The most frequently identified motivation (46%) in abuse cases was the convenience or availability of the computer for entertainment or personal/outside business.

The contrast between fraud and abuse cases in the judicial actions taken is not surprising given the survey definition that abuse "does not necessarily imply violation of a specific law." A more interesting finding is that 84 percent of the fraud cases and 70 percent of the abuse cases had some disciplinary or legal action taken, implying that a high proportion of perpetrators are indeed sanctioned. This bears closer examination in Phase II, since this finding could also be attributed to better documentation and recall in sanctioned cases.

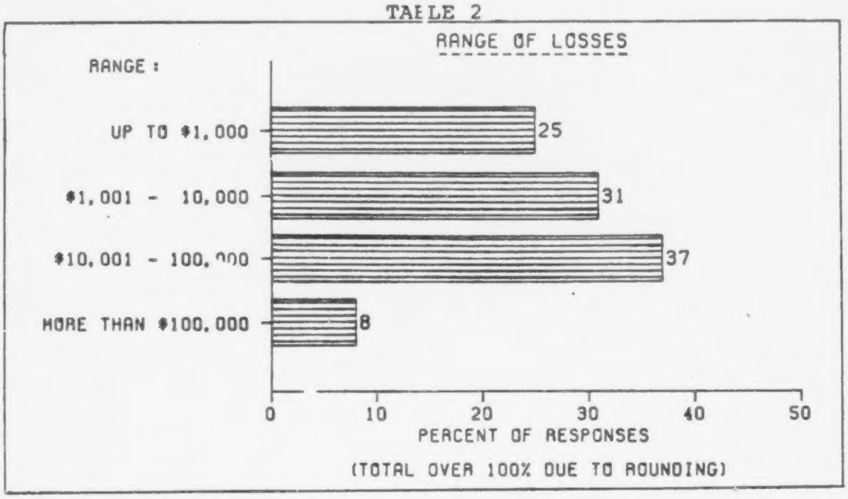
What Were the Losses Associated with Computer-Related Fraud and Abuse in this Study?

Respondents estimated losses in 58 percent of the total cases of fraud and abuse, ranging from $0 to $177,383. The responses for fraud versus abuse are as follows:

Fraud:

For the 65 cases in which data were provided, the responses ranged from $0 to $177,383 as follows:

TABLE 2



Respondents for fraud cases were also asked if they felt the loss figures they provided were lower than actual losses. Of the 61 responses, almost half (48%) stated they had reason to believe this amount was greater. For example:

> In one highly-publicized fraud of a benefit funds system, a claims technician created fictitious beneficiaries to obtain benefit payments for her co-conspirators. Although evidence used for prosecution established the amount of the fraud only as $102,000, investigators believe the perpetrator may have diverted as much as $500,000 through such fraudulent transactions.

Losses varied by the type of application system victimized. Almost three-fifths (59%) of the frauds occurred in benefit funds disbursement systems. Within benefit funds system cases, 63 percent of the individual losses were over $10,000. All of the cases with losses over $100,000 occurred in benefit funds disbursement systems. By contrast, payroll systems, which had the second highest (21%) incidence in our fraud cases, had most (78%) of the individual case losses in the range of $10,000 or less. (See page 13 for further discussion of contrasts between the two types of systems.)

Abuse:

Only 34 (33%) respondents in abuse cases gave estimates of monetary losses to their agencies, ranging from $0 to $5,214. The 33 percent included 17 percent who estimated no losses ($0), and 16 percent who estimated amounts greater than zero. Only 6 respondents gave estimates greater than $1,000.

Abuse respondents were also asked to estimate the value of any other losses, such as the value of stolen computer time, software, or data. Again, response was limited: 55 percent of the cases gave no estimate, 26 percent estimated $0, and the remaining 19 percent estimated between $2 and $3,500.

How Were the Cases Perpetrated?

The survey requested identification of the one or more techniques used to perpetrate the fraud or abuse. As shown below, respondents selected from 17 different techniques ranging from those related to input data to those related to development of programs or manipulation of processing. The following table displays the percentages of fraud and abuse cases in which each of the techniques was identified:

TABLE 3
Techniques Used to Perpetrate Computer-Related Fraud and Abuse

Technique	% Fraud*	% Abuse*
Introduction of unauthorized input data	64	50
Manipulation of authorized input data	59	15
Manipulation or use of files/records	36	16
Creation of unauthorized files/records	30	47
Override of internal controls	25	7
Diversion or manipulation of output	20	12
Manipulation of computer programs or documentation	16	8
Manipulation or use of processing	14	29
Manipulation of errors, exceptions, or rejects	9	2
Unauthorized use of passwords or billing accounting codes	9	22
Unauthorized transmission or interception of communications	7	9
Theft of equipment, software, data or computer time	7	55
Manipulation of communications facilities or processing	6	14
Willful damage, destruction or alteration of equipment, software or data	3	8
Development of programs for improper purposes	1	34
Unauthorized use of vendor utility programs	1	14
Willful denial of service	1	5

---

*Percentages total more than 100% since more than one technique could be chosen.

As illustrated, most fraud cases involved introduction/manipulation of input and/or creation/manipulation of files. In 70 percent of the fraud cases, more than one technique was identified. For example:

> Three data entry clerks, through access to a remote terminal, entered fictitious claims and subsequently deleted records of these transactions to obtain over $150,000 in Food Stamps. The techniques employed were manipulation of authorized input data, introduction of unauthorized input data, and manipulation of files/records.

The high incidence of input types of fraud corresponds to GAO's findings in their 1976 report; 62 percent of their cases involved fraudulent record initiation.[6]

Abuse cases identified the techniques of development of programs for improper use and theft of equipment, software, data or computer time in greater proportions than did fraud cases. This corresponds to the predominate nature of abuse cases, i.e., theft of computer time. It also appears congruent with the finding that more data processing personnel than functional users are involved in abuse cases. Data processing personnel are more likely to have the necessary technical skills with which to use the computer facilities and develop or manipulate programs.

Similar to fraud cases, 78 percent of the abuse cases identified more than one technique to perpetrate the abuse. As indicated by the percentages in the table, abuse cases often showed some combination of unauthorized input, creation of unauthorized files, development of programs, and/or theft of computer time. The following two examples illustrate multiple techniques:

> A computer programmer ran football pools on his agency's computer. To do this, he wrote a small program to compute odds, format and print schedules, and record bets; made unauthorized inputs; and created records and files for each pool.

> An engineer used his agency's computer facilities to m maintain the records of his after-hours business and to transmit data messages to his customers. Upon discovery, the perpetrator was able to delete or encrypt his files, preventing management from determining the extent of his abuse. The perpetrator's techniques included introduction of unauthorized input and files, use of processing, development of programs, use of passwords, unauthorized transmission of communications, and theft of computer time.

How Were the Cases Detected?

In order to determine how well internal control systems detect computer fraud and abuse, respondents were asked to identify the source of detection, and the major factor which triggered detection. For analysis purposes, the sources of detection listed in Section 5.1 and the trigger factors listed in 5.2 of the survey instrument were grouped as follows:

- Sources of Detection
  - Agency Personnel - senior and middle managers, data processing personnel, and co-workers. This group also includes two (2) perpetrators who confessed to fraud.
  - Professional Evaluators - internal agency auditors, external auditors (such as GAO auditors), computer security officers, program or functional evaluators, and agency staff investigating computer match "hits".
  - Other - recipients of Federal benefits, contractor or vendor suppliers, and law enforcement and other investigative staff.
- Trigger Factors
  - Accident - chance occurrences such as complaints, curiosity or revenge of informers, unusual activities of perpetrators.
  - Audit - routine internal audit, routine external audit, non-routine audit, and investigative or computer security reviews.
  - Controls - internal controls, unusual change in accounting/management reports, violation of computer security controls, and noncompliance with operating procedures.

Table 4 displays how the cases were detected, and Table 5 displays factors which triggered detection. For a further breakdown of the percentages contained in Table 4, see Appendix B.

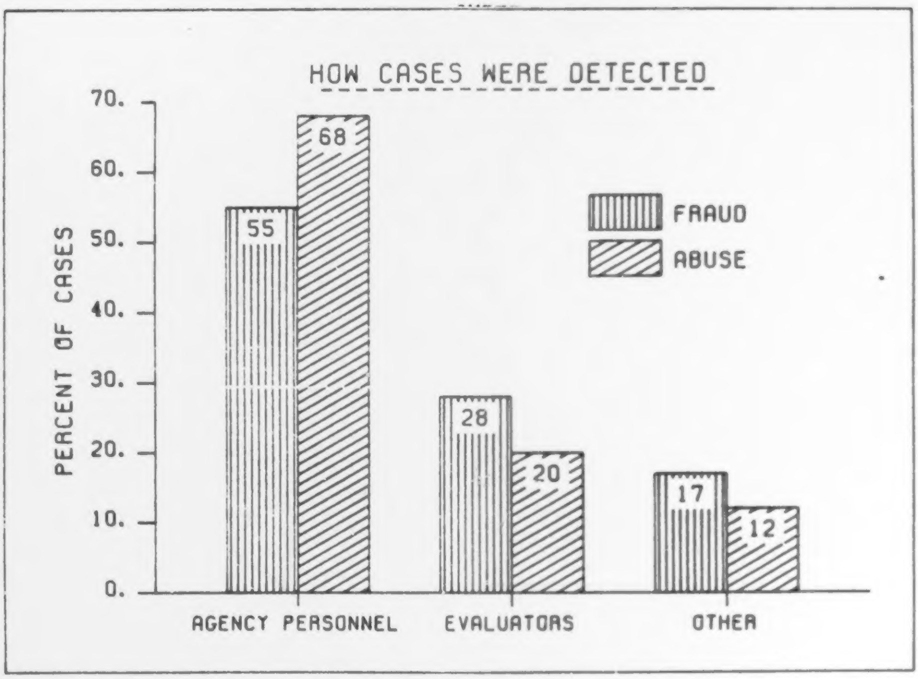
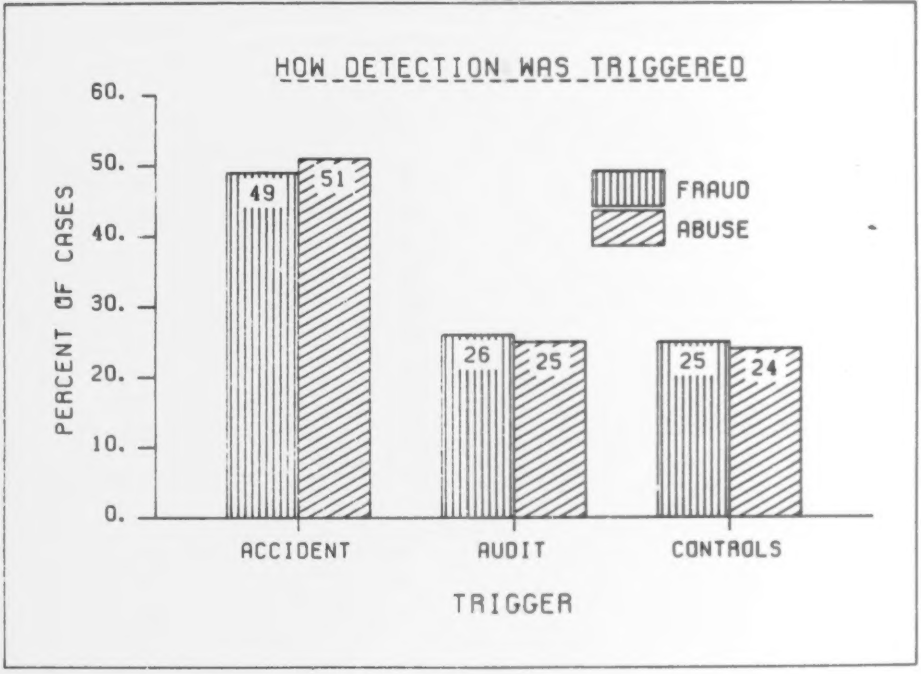

HOW CASES WERE DETECTED
PERCENT OF CASES
70.
60.
50.
40.
30.
20.
10.
0.
FRAUD
ABUSE
55
68
28
20
17
12
AGENCY PERSONNEL
EVALUATORS
OTHER

TABLE 5


HOW DETECTION WAS TRIGGERED
PERCENT OF CASES
60.
50.
40.
30.
20.
10.
0.
FRAUD
ABUSE
49
51
26
25
25
24
ACCIDENT
AUDIT
CONTROLS
TRIGGER

Most Cases Are Found Accidentally by Insiders

Agency personnel[8] detected more than one-half (55%) of the fraud cases and more than two-thirds (68%) of the abuse cases. Personnel in management positions discovered as many of the fraud cases (24%) as did co-workers (23%). However, co-workers identified more than twice as many abuse cases as did managers. Data processing personnel discovered a small percenage of the cases, but identified almost three times as many abuse as fraud cases. This is probably best explained by the fact that abuse cases involved mostly theft of computer time which data processing personnel would be alert to in conducting day-to-day activities. These personnel would less likely be alert to cases entailing fictitious benefits or unauthorized payroll payments.

In most cases, agency personnel discovered the cases by accident. In fact, an accidental occurrence triggered detection of twice as many cases as did either an audit or a system of control. Of the cases found by accident, most (27% fraud and 31% abuse) were triggered by chance or curiosity of the informer. For example:

> A Federal employee, through access to benefit claims authorization and input procedures, fraudulently obtained over $100,000 over 1½ years. He used the computer to reactivate accounts of deceased beneficiaries, and to create fictitious records. The case was detected by a bank clerk who observed the perpetrator opening more than one direct deposit account (in different names) at the same bank. The bank reported the observation to Federal officials.

The survey data show that only one-fourth of the cases (25% of fraud cases and 24% of abuse cases) were detected through internal controls. This finding indicates that agency control systems generally were nonexistent or inadequate to detect the cases at the time they were perpetrated.

Control systems were most effective, however, in detecting fraud cases involving payroll applications. Of the fraud cases entailing payroll, most (46%) were discovered through a control system, generally separation of duties. This contrasts markedly with the finding that only 12% of the cases involving fraud in benefit fund application systems were detected through controls. Most (59%) of the fraud cases involving benefit fund systems were discovered by accident. The vulnerability of benefit funds programs to fraud and abuse and the lack of control systems over them bears close scrutiny in Phase II of the project.

Professional evaluators identified about one-fourth of the cases (28% of fraud cases and 20% of abuse cases). Internal auditors comprised the largest percentage of evaluators and discovered most of their cases using traditional audit techniques. Internal auditors identified more fraud than abuse cases, detecting 27% of cases involving unauthorized payroll and 30% of cases involving benefit funds applications.

The survey data on how the cases were detected parallel those documented by other investigators. Parker[9] has reported that most cases of computer crime are detected by persons within the victimized organization. Also, GAO[10] documented that a high percentage of fraud (of all types) in government is detected by agency personnel. These sources also document that the preponderance of computer and white collar crimes are found by accident.

How Effective Were The Controls?

Questions pertaining to controls in the computer environment were asked to determine the proportion of cases in which controls were: not in place, in place but not used, or overridden. The questions were designed to identify how the lack of or weaknesses in control systems facilitated the fraud or abuse, and what controls should have been in place to prevent or trigger early detection of the case.

One-fifth of the respondents did not provide any information on system controls. The data provided in other cases were generally spotty and illogical when compared with the descriptions of the schemes involved. For example, a contractor employee was able to computer generate checks to herself by inputting false claims for medicare benefits. For more than three years, the perpetrator would input beneficiary names and identification data and her own address. Benefit checks were then sent to her home. The fraud was found by accident. Section 8.1 of the survey form indicated that controls were in place, and there were no recommendations with respect to controls that should have been in place or could be implemented to prevent or detect the fraud. It is illogical to believe that controls can be effectively in place and permit a fraudulent act to continue until it is found by accident.

The poor quality of the responses to questions on controls implies a lack of knowledge about computer system controls among respondents. It also implies that information on control systems generally is not documented during investigations. Hence, the data which was provided may be based, for the most part, on the respondent's memory of the case, or his ability to deduce the probable status of control systems from a description of the case. Whether or not a review of computer system controls is a part of the investigation of a computer crime is an issue to be explored in Phase II of the project.

Because of the non-comparability of the data requested and supplied, no attempt was made to summarize these responses for analysis purposes.

Many of the reported cases identified controls which were not in place, were not used, or were overridden. This apparent lack of good control systems across Federal agencies seems to explain the finding that most computer fraud and abuse cases were detected by accident, and the low incidence (25% fraud, 24% abuse) of cases detected through controls. A good system of controls would have prevented the cases or have led to their early detection. The following cases illustrate the lack of or weaknesses in control systems.

Controls Not in Place or Overridden

- The lack of procedures requiring segregation of duties, and the lack of forms control made it possible for a Federal employee to establish unauthorized benefit claims and divert $24,000 over a 5-month period. The perpetrator was able to change information in a deceased client's file. The perpetrator was also able to correct his input errors because no segregation of duties existed in the edit resolution, and his corrective inputs were not reviewed by a supervisor. After a check was generated, the perpetrator was able to erase erroneous data. Eventually the case was detected by a computer match and subsequent investigation.
- In another case, the lack of segregation of duties and the ability to override input controls permitted a Federal employee to redirect program recoveries to his own bank account. The perpetrator was able to clear a systems alert code, delete a notice of recovery, and steal the repayment. There was no system of review to assure proper posting of recoveries. This fraudulent act went undetected until a fellow employee accidently noticed the improper processing of cases and notified management.

Controls Not Used

- A caseworker created fictitious applications for Food Stamps. She entered the fictitious information in the computer to generate authorizations to purchase Food Stamps, which she then received and cashed. Although there were procedures to assure supervisory review of new applications and authorization of new transactions, the procedures were not followed. The case was detected accidently by a co-worker. The estimated loss in the case exceeded $12,000.

- Three data entry clerks were able to steal Food Stamps, valued at over $150,000, because the supervisor consistently left his key in the issuance terminal. The clerks stole the Food Stamps and used the computer to generate false issuance reports by deleting their personal "transactions" from the file. Written procedures requiring authorization of transactions, management review, and input controls were not used by the supervisor. The supervisor's failure to control access to the issuance terminal also violated agency policy.

In addition to identifying general controls in the computer environment, respondents were asked whether agency computer systems were subject to any type of audit or review. Also, they were asked whether a formal risk analysis/vulnerability assessment program had been implemented in accordance with OMB Circulars A-71 and A-123. Transmittal Memorandum No. 1 to OMB Circular A-71 (July 27, 1978) requires Federal agencies to establish automated security programs, and A-123 requires each agency to establish and maintain adequate systems of internal controls.

Responses to these questions were very weak. In more than three-fourths (78%) of the cases, respondents were unable to answer the questions concerning a system audit or review, and over two-thirds (68%) lacked knowledge about the implementation of A-71 and A-123. These data support our earlier finding that the lack of and weaknesses in controls exist in computer environments. Further, the paucity of responses to these questions indicates a general lack of awareness among respondents about internal controls or where to turn for information about those controls.

CONCLUSIONS AND RECOMMENDATIONS

Despite the constraints mentioned in the Findings Section, the data do provide a picture of the type of computer-related fraud and abuse which is known to and reported by the Inspector General community. The frauds are characterized by low level employees in functional areas committing input types of frauds in Government payment systems. The abuses usually involve higher paid, technically sophisticated employees using computer resources. Both types of acts are usually detected accidentally by insiders.

Further Survey Work

Although this picture is possible from the data, we cannot determine the scope of the problem of computer-related fraud and abuse in Government. In addition to the problems regarding lack of a systematic case identification, other factors work against a complete picture of computer-related fraud and abuse. The literature discusses both the weaknesses in controls (and therefore in detection capabilities) and the reluctance of officials of victimized systems to report computer-related fraud or abuse once detected. Such factors may account for the relatively low number of responses, given the existence of over 16,000 computerized systems.

In addition, certain portions of the survey responses are incomplete, particularly in the areas of loss estimates, knowledge of prior audits or reviews, and systems controls. Nevertheless, because this survey is the first of its type in Government, we need to refine and maintain it as a unique source of information for the IG community. Therefore, because we must assess the limits of the survey data and build upon it as an ongoing source of information and analyses, we recommend the following:

- The Computer Security Task Force should conduct Phase II to identify and analyze the causes of the survey data limitations, the extent of computer security awareness and activity within the IG organizations, and the state of controls in victimized systems. The specific objectives of Phase II should include the following:

  --To identify cases which were not identified or reported in the survey and assess reasons for unreported cases.

  --To ascertain the reasons for incomplete responses in such areas as controls, prior audits and reviews, and loss.

  --To determine why no cases were reported by some agencies (e.g., because of better controls, lack of investigative jurisdiction, etc.).

  --To collect best practices in the vulnerability/risk assessment programs implemented per OMB Circulars A-71 (Transmittal Memorandum No. 1) and A-123.

  --To determine agency and OIG experience with detection and investigation of computer-related incidents.

- Once Phase II is complete, the task force should conduct periodic survey updates to build upon the initial survey data and experience, to maintain awareness in the IG community, and to keep the Council informed of the extent of the known problem. This update should utilize the new FACTS and Secret Service information systems, as well as sources identified through Phase II.

Training and Awareness

The incomplete responses on systems controls and prior audits or reviews point to the likely explanation that the respondents, who were mostly investigators, had no knowledge of these areas. Investigators, whether in the IG environment or in agency integrity/security functions, are not usually as involved as auditors in the identification of internal controls. Similarly, investigators may not be as aware of documented systems control weaknesses, if in fact such audits or reviews exist.

Conversely, however, investigators should be aware of exploited vulnerabilities through their investigations, and should be recommending systemic improvements based on their case experience. This integration of investigative experience into program improvement recommendations is becoming increasingly common in IG organizations. It appears from our survey responses, however, that investigators are not aware of the state of internal controls in their agencies' computerized systems, nor possibly about the types of controls necessary to automated systems in general. While this lack of awareness needs confirmation through the Phase II followup, such conclusions are reinforced by anecdotal information. A number of respondents commented that the PCIE survey had heightened their awareness of computer weaknesses and the need to know more about controls.

From these preliminary findings and conclusions, then, it would appear that training of investigative staff on controls in automated systems (particularly payment systems) and in the findings of any specific computer audits, vulnerability assessments, or security reviews in their agencies would improve both the investigative process through recognition of known vulnerabilities and the investigators' input to recommendations for systems improvements. Any such training and awareness programs should be integrated with the PCIE Computer Audit Council curricula now being developed for auditors and investigators. Therefore, we recommend that:

- IGs should provide training, such as the curricula being developed by the PCIE Computer Audit Council, to investigators, as well as auditors, on the internal controls in automated systems.

- Investigators should be made aware of the documented vulnerabilities of their agencies' computer systems, including the results of EDP audits and internal control reviews.

Controls in Automated Systems

Although the PCIE survey responses provide insufficient data to identify specific control weaknesses in the victimized systems, the findings, especially those regarding detection, do imply that systems and management controls are inadequate, as has been discussed in numerous prior reports. Individual cases do show that controls can be effective in the detection of computer-related fraud and abuse. The aggregate data, however, show that half of the cases were detected by accident. The finding is alarming because of the implications for both control weaknesses and undetected fraud and abuse.

Cases in the survey data base occurred during the time frame from 1978 to 1982. While the concern about the vulnerabilities of computerized systems has not lessened since then, the requirements of OMB Circulars A-71 (Transmittal Memorandum No. 1) and, especially, A-123, which was only issued October 28, 1981, were not fully implemented at the time these computer-related frauds and abuses occurred. The requirements for computer security and internal controls provide the framework and processes through which agencies can identify the types of systems and management control weaknesses which were exploited in many of the survey cases. Therefore, although we cannot address either specific or current control weaknesses without further review, we do recommend the following:

- Agencies, in their A-123 internal control reviews, should give particular emphasis to assessments of the internal controls in automated systems. In light of the survey findings on computer-related fraud, payment systems appear most vulnerable and should be given especially close scrutiny.

- The PCIE should establish a system to alert all IG and related organizations to generic computer system control weaknesses and vulnerabilities found during investigations, audits or reviews. Such a system would serve in concert with the ongoing data collection and internal training and awareness recommendations to focus the IG community on common systems weaknesses and enable them to devise common prevention strategies.

FOOTNOTES:

[1] U. S. Congress, Senate, Committee on Government Operations, Staff Study of Computer Security in Federal Programs, (Washington, D.C.: U. S. Government Printing Office, February 1977), p. 267.

[2] U. S. Department of Justice, Law Enforcement Assistance Administration, Computer Crime: Criminal Justice Resource Manual, by SRI International, under Grant No. 78-SS-AX-0031, (Washington, D.C.: U. S. Government Printing Office, 1979), p. 2.

[3] U. S. Congress, General Accounting Office, Federal Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices, (MASAD-82-18, April, 1982), p. 7.

[4] U. S. Congress, General Accounting Office, Computer-Related Crimes in Federal Programs, (FGMSD-76-27, April 27, 1976), p. 2.

[5] Percentages are given for the total responses present on each item. The proportion of missing responses is less than 10 percent in all characteristics except salary (fraud). Data were unavailable in 16 percent of the fraud cases on this characteristic.

[6] U. S. Congress, General Accounting Office, Computer-Related Crimes in Federal Programs, (FGMSD-76-27, April 27, 1976), p. 6.

[7] Respondents frequently characterized co-workers as whistleblowers.

[8] Agency personnel includes mostly Federal workers (74%).

[9] Donn Parker and Susan Nycum, "Computer Crimes: Case Histories and Proposed Legislation," report prepared for the HEW Secretary's National Conference on Fraud, Abuse, and Error, December 1978, p. 6.

[10] U. S. Congress, General Accounting Office, Fraud in Government Programs--How Extensive Is It?--How Can It Be Controlled?, (AFMD-81-57, May 7, 1981), p. 20.

Appendix A

PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY

COMPUTER SECURITY PROJECT

Survey of Computer-Related Fraud and Abuse

1.0 INTRODUCTION

The President's Council on Integrity and Efficiency recognizing the critical role of the computer in the administration of government programs, is sponsoring an in-depth study of computer-related fraud and abuse in the Federal sector. The study reflects the concern contained in GAO and other official reports about the lack of controls in Federal automated systems. The objective of the study is to provide the Council a perspective on the nature of computer-related fraud and abuse cases in Federal programs, and, thereby, a perspective on techniques, controls and resources needed to combat such activity. The study will be limited to fraud and abuse cases which were discovered between January 1, 1978 and March 31, 1982.

As part of the study, this survey form has been developed to elicit information regarding computer-related fraud and abuse, and methods used to detect, deter, and prevent it.

1.1 Confidentiality of Survey Responses

To assure confidentiality, the specific findings and analyses from this survey will not be attributed to any Federal Department or Agency in the final report on this Council project.

1.2 Definitions

1.2.1 Computer-related fraud is any illegal intentional act or series of acts, that is designed to deceive or misrepresent in order to obtain something of value. Further, a computer system must have been involved in the perpetration or cover-up of the act, or series of acts. A computer system might have been involved through improper manipulation of: (1) input or transaction data, (2) output or results, (3) application programs, (4) data files, (5) computer operations, (6) communications, or (7) computer hardware, systems software, or firmware.

1.2.2 Computer-related abuse is the misuse, destruction, alteration or disruption of data processing resources. The key aspects of computer-related abuse are that it is intentional and improper, but it does not necessarily imply the violation of a specific law nor the presence of false representation. Examples of computer-related abuse are, (a) unauthorized use of the computer by Federal employees for their personal programming activities, and (b) misuse of computer equipment for revenge against a government agency.

If you are not sure whether your case fits these definitions, fill out the form as best you can.

1.3 Instructions

Please complete Sections 2.0 through 9.0 for each case of computer-related fraud or abuse which has been discovered in your Department/Agency, between January 1, 1978 and March 31, 1982. A case, for purposes of this survey, is any situation where an individual (or group of individuals) has been alleged to or proven guilty of having committed computer-related fraud or abuse.

Please return all survey forms no later than June 16, 1982

If you have questions about the Council project or the survey form, please call one of the following:

Sheila Brand, DoD	(301) 859-6818
Dale Steward, DOC	(202) 376-7670
Jane Tebbutt, HHS	(202) 472-5340

Mail completed surveys to:

COMPUTER FRAUD AND ABUSE SURVEY (OSI)
Room 5246, HHS (OIG)
Washington, DC 20201

2.0 TYPE OF COMPUTER-RELATED FRAUD OR ABUSE

2.1 Using the definitions in the instructions to this survey form, please identify, with a check in the appropriate box, whether this case was:

- 2.1.1 ☐ Computer-related fraud, or
- 2.1.2 ☐ Computer-related abuse.

2.2 What was the nature of the case? (Check all that apply)

- 2.2.1 ☐ Theft of cash or diversion of other assets
- 2.2.2 ☐ Theft of computer time
- 2.2.3 ☐ Theft of hardware
- 2.2.4 ☐ Theft of software
- 2.2.5 ☐ Theft of data
- 2.2.6 ☐ Destruction or alteration of hardware
- 2.2.7 ☐ Destruction or alteration of software
- 2.2.8 ☐ Destruction or alteration of data
- 2.2.9 ☐ Denial of service (i.e. making computer resources unavailable for authorized use)

2.3 If this was a case of computer-related fraud proceed to 2.4. However, if this was a case of computer-related abuse involving the theft, destruction, or alteration of data identify whether the data were (check all that apply):

- 2.3.1 ☐ Officially specified "For Internal Use Only"
- 2.3.2 ☐ Subject to security classifications (e.g., confidential, secret, top secret, etc.)
- 2.3.3 ☐ Subject to provisions of the Privacy Act of 1974
- 2.3.4 ☐ Administrative data
- 2.3.5 ☐ Scientific/engineering data
- 2.3.6 ☐ Economic data (commodities, futures, etc.)
- 2.3.7 ☐ Other, please specify:

2.4 Additional Comments

1.0 PERPETRATOR PROFILE(S)

How many individuals were involved in the fraud or abuse? _____

Please provide on the following four pages requested information on each individual (up to four) who played an instrumental role in committing the fraud or abuse. Fill in the perpetrator profile in the order of individual importance with number one being the leader. If, after filling in sections 3.1 through 3.4 you believe additional perpetrator profile detail is needed to understand the case, please provide it below.

3.1 Perpetrator Number One

3.1.1 Position/job title: ______________________________

3.1.2 Position type: [ ] Clerical [ ] Professional

3.1.3 Position level: [ ] Nonsupervisory [ ] Supervisory
[ ] Management

3.1.4 Employer: [ ] U.S. Government
[ ] State/Local Government
[ ] Private Industry

3.1.5 Estimated Salary per yr: [ ] Less than $10,000
[ ] $10,000 to $20,000
[ ] $20,001 to $35,000
[ ] $35,001 to $50,000
[ ] More than $50,000

3.1.6 Length of service/relationship with Agency:

[ ] Less than 1 yr. [ ] 1-5 yrs. [ ] 5-10 yrs.
[ ] 10-20 yrs. [ ] More than 20 yrs.

3.1.7 Individual's primary motive:

Please indicate disciplinary and legal actions taken against the individual (Check all that apply):

3.1.8 [ ] None
3.1.9 [ ] Letter of reprimand
3.1.10 [ ] Suspended (Length: __________)
3.1.11 [ ] Resigned under duress
3.1.12 [ ] Dismissed from employment
3.1.13 [ ] Judicial action pending
3.1.14 [ ] Indicted (Statute(s): __________________)
3.1.15 [ ] Convicted (Statute(s): __________________)
3.1.16 [ ] Sentenced (Length: ________________)
3.1.17 [ ] Fined (Amount: _____________)
3.1.18 [ ] Restitution required (Amount: ____________)
3.1.19 [ ] Other penalties, describe:

3.2 Perpetrator Number Two

3.2.1 Position/job title: ______________________________

3.2.2 Position type: ☐ Clerical ☐ Professional

3.2.3 Position level: ☐ Nonsupervisory ☐ Supervisory
☐ Management

3.2.4 Employer: ☐ U.S. Government
☐ State/Local Government
☐ Private Industry

3.2.5 Estimated salary per yr: ☐ Less than $10,000
☐ $10,000 to $20,000
☐ $20,001 to $35,000
☐ $35,001 to $50,000
☐ More than $50,000

3.2.6 Length of service/relationship with Agency:

☐ Less than 1 yr. ☐ 1-5 yrs. ☐ 5-10 yrs.
☐ 10-20 yrs. ☐ More than 20 yrs.

3.2.7 Individual's primary motive:

Please indicate disciplinary and legal actions taken against the individual (Check all that apply):

3.2.8 ☐ None
3.2.9 ☐ Letter of reprimand
3.2.10 ☐ Suspended (Length:__________)
3.2.11 ☐ Resigned under duress
3.2.12 ☐ Dismissed from employment
3.2.13 ☐ Judicial action pending
3.2.14 ☐ Indicted (Statute(s) ____________________)
3.2.15 ☐ Convicted (Statute(s)____________________)
3.2.16 ☐ Sentenced (Length: ________________)
3.2.17 ☐ Fined (Amount: ______________)
3.2.18 ☐ Restitution required______ (Amount: ______________)
3.2.19 ☐ Other penalties, describe:

3.3 Perpetrator Number Three

3.3.1 Position/job title: ______________________________

3.3.2 Position type: ☐ Clerical ☐ Professional

3.3.3 Position level: ☐ Nonsupervisory ☐ Supervisory
☐ Management

3.3.4 Employer: ☐ U.S. Government
☐ State/Local Government
☐ Private Industry

3.3.5 Estimated salary per yr: ☐ Less than $10,000
☐ $10,000 to $20,000
☐ $20,001 to $35,000
☐ $35,001 to $50,000
☐ More than $50,000

3.3.6 Length of service/relationship with Agency:

☐ Less than 1 yr. ☐ 1-5 yrs. ☐ 5-10 yrs.
☐ 10-20 yrs. ☐ More than 20 yrs.

3.3.7 Individual's primary motive:

Please indicate disciplinary and legal actions taken against the individual (Check all that apply):

3.3.8 ☐ None
3.3.9 ☐ Letter of reprimand
3.3.10 ☐ Suspended (Length:__________)
3.3.11 ☐ Resigned under duress
3.3.12 ☐ Dismissed from employment
3.3.13 ☐ Judicial action pending
3.3.14 ☐ Indicted (Statute(s)________________________)
3.3.15 ☐ Convicted (Statute(s)________________________)
3.3.16 ☐ Sentenced (Length: ________________)
3.3.17 ☐ Fined (Amount: ________________)
3.3.18 ☐ Restitution required (Amount: ____________)
3.3.19 ☐ Other penalties, describe:

3.4 Perpetrator Number Four

3.4.1 Position/job title: ______________________________

3.4.2 Position type: ☐ Clerical ☐ Professional

3.4.3 Position level: ☐ Nonsupervisory ☐ Supervisory
☐ Management

3.4.4 Employer: ☐ U.S. Government
☐ State/Local Government
☐ Private Industry

3.4.5 Estimated salary per yr: ☐ Less than $10,000
☐ $10,000 to $20,000
☐ $20,001 to $35,000
☐ $35,001 to $50,000
☐ More than $50,000

3.4.6 Length of service/relationship with Agency:

☐ Less than 1 yr. ☐ 1-5 yrs. ☐ 5-10 yrs.
☐ 10-20 yrs. ☐ More than 20 yrs.

3.4.7 Individual's primary motive:

Please indicate disciplinary and legal actions taken against the individual (Check all that apply):

3.4.8 ☐ None
3.4.9 ☐ Letter of reprimand
3.4.10 ☐ Suspended (Length: __________)
3.4.11 ☐ Resigned under duress
3.4.12 ☐ Dismissed from employment
3.4.13 ☐ Judicial action pending
3.4.14 ☐ Indicted (Statute(s) ________________________)
3.4.15 ☐ Convicted (Statute(s) ________________________)
3.4.16 ☐ Sentenced (Length: ______________)
3.4.17 ☐ Fined (Amount: ______________)
3.4.18 ☐ Restitution required (Amount: ______________)
3.4.19 ☐ Other penalties, describe:

4.0 DESCRIPTION OF THE CASE

4.1 In what agency and program was the fraud or abuse perpetrated?

4.2 How was the fraud or abuse perpetrated? If collusion was involved be sure to describe it.

4.3 How was the fraud or abuse concealed?

4.4 How was the fraud or abuse discovered?

4.5 How was the computer system involved?

4.6 Over what period of time did the fraudulent or abusive act occur?

Began ______ ______ Stopped ______ ______
month year month year

4.7 Approximately how many times did the fraudulent or abusive action take place in this period of time?

4.8 If this case was computer-related fraud, please answer questions 4.8.1 through 4.8.4, providing exact dollar amounts if known, otherwise giving your best estimates. If this is not a case of computer-related fraud, go to 4.9.

4.8.1 What was the total known dollar loss to the agency?

$____________
(amount)

4.8.2 Do you have reason to believe that the amount was greater than this, even though it cannot be definitely determined?

☐ Yes ☐ No

4.8.3 How much of the loss actually was converted to cash or other assets and extracted from the agency?

$____________
(amount)

4.8.4 How were the funds or other assets extracted from the agency?

Please go to question 4.10.

4.9 If this was computer-related abuse, please provide the following information:

4.9.1 The exact dollar amount or your best estimate of any monetary loss to your agency. Include actual cash loss, computer down time, cost of recovery or replacements, etc.

$__________
(amount)

4.9.2 The value of any other losses. (For example, estimate the value of stolen computer time, software, or data.)

$__________
(amount)

4.10 Additional comments

5.0 HOW THE FRAUD OR ABUSE WAS DETECTED

5.1 Who first detected the irregularity?

5.1.1 [ ] Internal Auditor (e.g., IG, US Army Audit Agency, etc.)
5.1.2 [ ] External Auditors (e.g., GAO, CPA Firm, etc.)
5.1.3 [ ] Senior Management
5.1.4 [ ] Middle Management
5.1.5 [ ] Computer/Security Officer
5.1.6 [ ] Program/Functional Evaluator
5.1.7 [ ] Data Processing Personnel
5.1.8 [ ] Recipient of Federal Benefits
5.1.9 [ ] Contractor/Vendor/Supplier
5.1.10 [ ] Whistleblower
5.1.11 [ ] Perpetrator (Turned self in)
5.1.12 [ ] Law Enforcement or Investigator
5.1.13 [ ] Computer Match
5.1.14 [ ] Other (please specify)

5.2 What major factor triggered the detection of the fraud or abuse? (check only one)

5.2.1 [ ] Routine Internal Audit
5.2.2 [ ] Routine External Audit
5.2.3 [ ] Internal Controls
5.2.4 [ ] Non-Routine Audit
5.2.5 [ ] Investigation or Computer Security Review
5.2.6 [ ] Unusual Change in Accounting/Management Reports
5.2.7 [ ] Complaint of Recipient or Vendor
5.2.8 [ ] Violation of Computer Security Controls

5.2.9 ☐ Change in/damage to computer systems (e.g., service, equipment, software, data)

5.2.10 ☐ Change in or non-compliance with operating procedures

5.2.11 ☐ Unusual activities or living habits of perpetrators

5.2.12 ☐ Guilt feelings of perpetrator(s)

5.2.13 ☐ Curiosity of informer

5.2.14 ☐ Revenge of informer

5.2.15 ☐ Hotline Complaint

5.2.16 ☐ Accident

5.2.17 ☐ Change in individual responsibilities (e.g., reorganization, reassignment, promotion)

5.2.18 ☐ Other (please specify)

5.3 Please explain how the item checked in section 5.2 helped to trigger the detection.

5.4 Additional Comments

6.0 COMPUTER ENVIRONMENT

For the following four questions, please provide answers only for the aspect of the computer environment relevant to fraudulent or abusive activity.

6.1 Which of the following describes the computer environment involved?

6.1.1 ☐ In-house facility (agency operated)
6.1.2 ☐ Facility operated by another agency
6.1.3 ☐ Federally-owned contractor-operated
6.1.4 ☐ Facilities management contract
6.1.5 ☐ Contractor owned-contractor operated
6.1.6 ☐ Commercial service bureau
6.1.7 ☐ Commercial time-sharing service
6.1.8 ☐ State/local facility
6.1.9 ☐ Other (please specify)

6.2 Which of the following describes the general computer technology employed relevant to the case? (Check all that apply.)

6.2.1 ☐ On-line, real-time processing
6.2.2 ☐ On-line inquiry
6.2.3 ☐ Remote batch
6.2.4 ☐ Batch processing
6.2.5 ☐ Centralized processing
6.2.6 ☐ Distributed processing
6.2.7 ☐ Data base management system
6.2.8 ☐ Other (please specify)

6.3 What was the general functional application in which the scheme occurred (e.g., payroll, accounting, personnel, supply, maintenance, benefit funds disbursements, scientific, etc.) Check whether the systems were substantially developed in-house or by contractor.

Functional Application System	Developed In-House	Developed by Contractor	Estimated Number of Master Records	Estimated Number of Transactions Per Month
	☐	☐		
	☐	☐		
	☐	☐		
	☐	☐		

6.4 Were any computer programs developed or modified specifically for the purpose of performing or concealing the fraudulent or abusive activity.

Yes ☐ No ☐ Not known ☐

6.4.1 If yes, describe

6.5 Additional Comments

7.0 METHODS EMPLOYED TO PERPETRATE AND CONCEAL THE FRAUD OR ABUSE

7.1 At what stage of the system procurement, development or operation, was the fraud or abuse perpetrated and or concealed? Check all that apply.

7.1.1 ☐ Application Design/Development/Testing

7.1.2 ☐ Normal Processing

7.1.3 ☐ Application Program Maintenance

7.1.4 ☐ Operating System Maintenance

7.1.5 ☐ Equipment Acquisition/Testing/Maintenance

7.1.6 ☐ Other (please specify)

7.2 What techniques were employed to perpetrate and/or conceal the fraudulent activity or cause the computer abuse? Check all that apply.

	Perpetrate	Conceal	
7.2.1	☐	☐	Manipulation of authorized input data
7.2.2	☐	☐	Introduction of unauthorized input data
7.2.3	☐	☐	Manipulation of errors, exceptions, or rejects
7.2.4	☐	☐	Override of internal controls
7.2.5	☐	☐	Manipulation or use of processing
7.2.6	☐	☐	Diversion or manipulation of output
7.2.7	☐	☐	Manipulation or use of files/records
7.2.8	☐	☐	Creation of unauthorized files/records
7.2.9	☐	☐	Manipulation of computer programs or documentation
7.2.10	☐	☐	Development of programs for improper purposes
7.2.11	☐	☐	Use of passwords or billing accounting codes
7.2.12	☐	☐	Use of vendor utility programs

	Perpetrate	Conceal	
7.2.13	☐	☐	Manipulation of communications facilities or processing
7.2.14	☐	☐	Unauthorized transmission or interception of communications
7.2.15	☐	☐	Theft of equipment, software, data or computer time
7.2.16	☐	☐	Willful damage, destruction or alteration of equipment software or data
7.2.17	☐	☐	Willful denial of service

7.2.18 Other (please specify)

7.3 Additional comments

8.0 EFFECTIVENESS OF CONTROLS AND AUDIT PROCEDURES

8.1 Please identify which of the following general controls were contained in the computer environment that was subject to the fraud or abuse. Check only one box per control.

		In Place and Used	Not In Place	In Place Not Used	In Place Overridden
8.1.1	Segregation of duties	☐	☐	☐	☐
8.1.2	Written procedures	☐	☐	☐	☐
8.1.3	Authorization of transactions	☐	☐	☐	☐
8.1.4	Forms control	☐	☐	☐	☐
8.1.5	Input controls	☐	☐	☐	☐
8.1.6	Source documents control	☐	☐	☐	☐
8.1.7	Error/reject controls	☐	☐	☐	☐
8.1.8	Physical access controls to ADP	☐	☐	☐	☐
8.1.9	Data validation	☐	☐	☐	☐
8.1.10	Computer system automated access controls (e.g., passwords)	☐	☐	☐	☐
8.1.11	Management and technical review/sign-off of program changes	☐	☐	☐	☐
8.1.12	Systems documentation	☐	☐	☐	☐
8.1.13	Transaction audit trails and balancing	☐	☐	☐	☐
8.1.14	Output distribution controls	☐	☐	☐	☐
8.1.15	Operation/production controls	☐	☐	☐	☐
8.1.16	Master file controls	☐	☐	☐	☐
8.1.17	Library controls	☐	☐	☐	☐

8.1.18 Program version controls	☐	☐	☐	☐
8.1.19 Other (please specify)				

8.2 What responsibilities, duties, or information relevant to the fraud or abuse did the perpetrator(s) have that enabled him/her to perpetrate or conceal the action?

8.3 In your opinion, what controls could prevent a recurrence of a similar case of fraud or abuse.

8.4 In your opinion, what controls could detect a recurrence of a similar case?

8.5 Was the computer system audited/reviewed during the period in which the fraud or abuse occurred?

Yes [ ] No [ ] Don't Know [ ]

If you checked the YES box, answer questions 8.5.1 through 8.5.5, otherwise go to question 8.6.

8.5.1 Who (GAO, OIG, Agency Management, etc.) performed the audit/review? ____________________

8.5.2 Did the audit/review address the area in which the fraud or abuse occurred?

Yes [ ] No [ ] Don't Know [ ]

8.5.3 Did the audit/review detect general problem(s) but not identify it(them) as a fraud or abuse?

Yes [ ] No [ ] Don't Know [ ]

8.5.4 Did the audit/review address computer controls?

Yes [ ] No [ ] Don't Know [ ]

8.5.5 Were computer-assisted techniques (computer matching, automated data analysis, monitors, etc.) employed during the audit/review?

Yes [ ] No [ ] Don't Know [ ]

8.6 Was a formal risk assessment program in place in accordance with OMB Circulars A-71 or A-123.

Yes [ ] No [ ] Don't Know [ ]

8.7 What procedures/controls would have detected the fraud or abuse?

8.8 Additional comments:

9.0 Council Follow-up Action

It may be necessary that we obtain clarifying or additional information from you to ensure that our analysis of cases is developed accurately. Accordingly, please provide the information requested below. To ensure confidentiality, ownership of the data supplied through this survey belongs to and will remain with the Department/Agency which completes the form. Any questions which might arise from outside sources with regard to information supplied by a particular Department/Agency will be referred to that Department/Agency. Further, specific findings and analyses from this survey will not be attributed to any Federal Department or Agency in the final report.

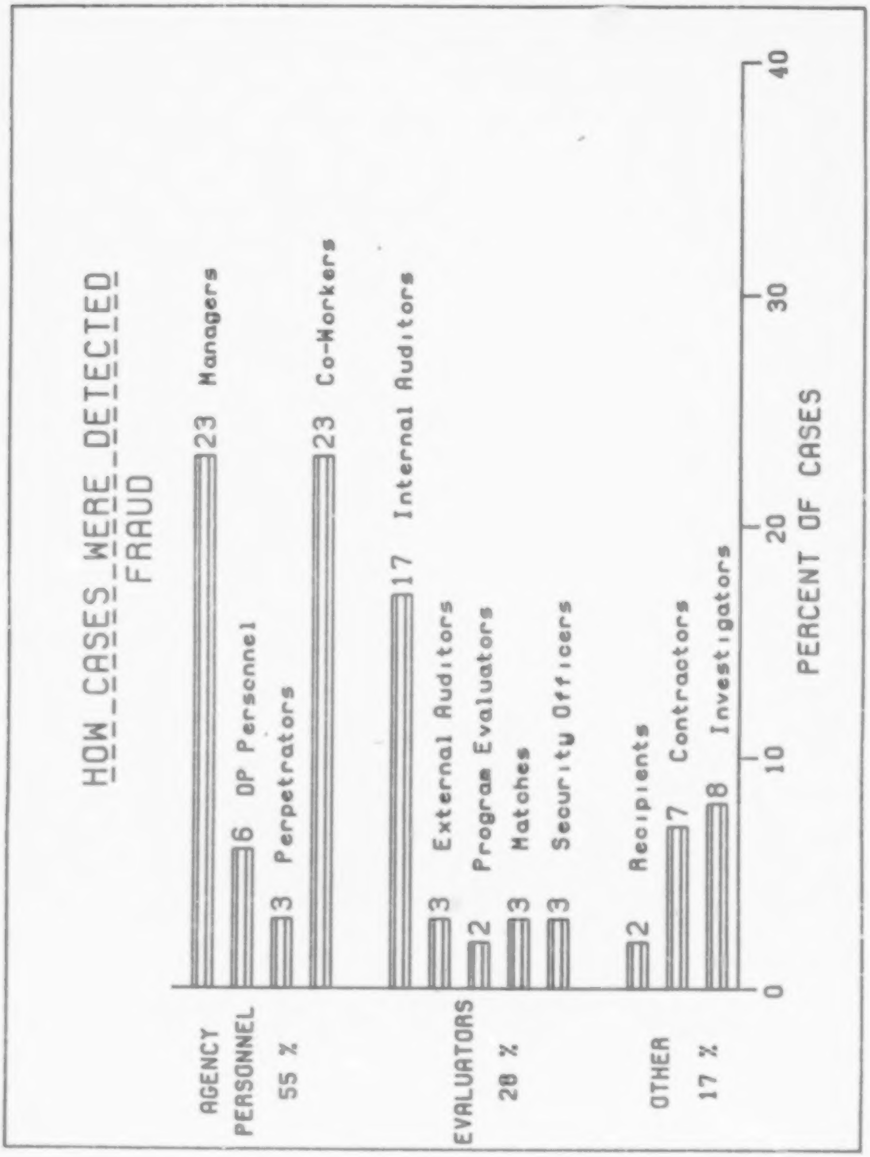
9.1 Department/Agency ______________________

9.2 Address ______________________

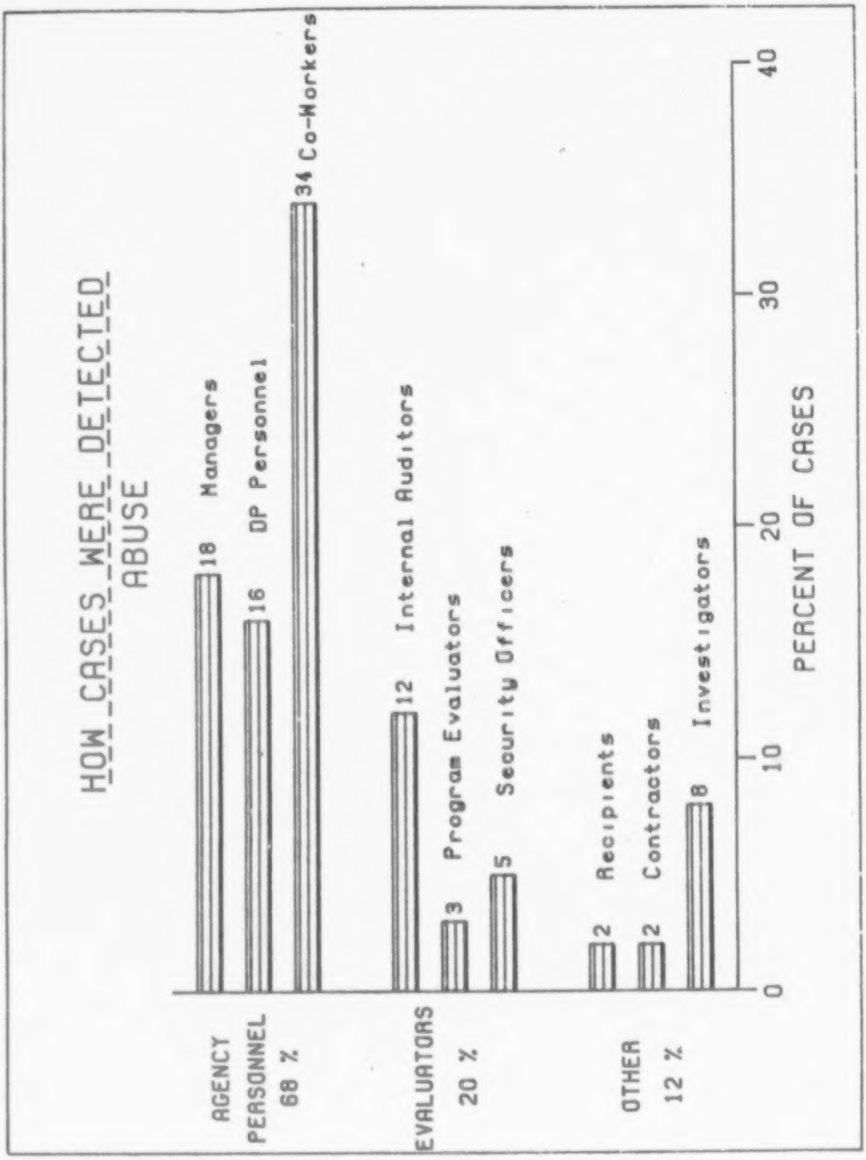
9.3 Contact Person for this case ______________________

9.4 Telephone Number ______________________

Appendix B


HOW CASES WERE DETECTED
FRAUD
AGENCY PERSONNEL 55 %
23 Managers
6 DP Personnel
3 Perpetrators
23 Co-Workers
EVALUATORS 28 %
17 Internal Auditors
3 External Auditors
2 Program Evaluators
3 Matches
3 Security Officers
OTHER 17 %
2 Recipients
7 Contractors
8 Investigators
0
10
20
30
40
PERCENT OF CASES

B -2


HOW CASES WERE DETECTED
ABUSE
AGENCY PERSONNEL 68 %
18 Managers
16 DP Personnel
34 Co-Workers
EVALUATORS 20 %
12 Internal Auditors
3 Program Evaluators
5 Security Officers
OTHER 12 %
2 Recipients
2 Contractors
8 Investigators
0
10
20
30
40
PERCENT OF CASES

1. Q: "You indicated in your October 17, 1983 testimony that OMB is responsible for coordinating Federal information security activities but that a major part of this responsibility is shared by the agencies. Please explain the division of responsibilities."

   A: OMB Circular No. A-71 defines the division of responsibility for computer security. It places prime responsibility for establishing a computer security program on the head of each agency. In addition, it gives OMB an oversight role and assigns to the Department of Commerce, the General Services Administration, and the Office of Personnel Management (the Civil Service Commission when the Circular was issued), certain government-wide responsibilities for computer security that are consistent with their expertise. A copy of that Circular is attached as well as a listing of the policy issuances of the central management agencies.

2. Q: "What actions did OMB take in following agencies' compliance with Circular A-71, Transmittal Memorandum No. 1.? Please provide results and dates."

   A: In December of 1978, OMB convened a small task force consisting of knowledgeable personnel from various agencies, to evaluate agencies' plans for implementing computer security programs submitted in response to the requirements of TM No. 1.

   Because of variances in the plans received, the task force developed and sent to the agencies a checklist of what should be in a good computer security program to assist them in developing their own plans. Plans already received were evaluated for conformance with the checklist criteria and those that were inadequate were returned to the agencies for reworking. This occurred early in 1979. Revised plans were to be submitted by the end of February 1979.

   Following resubmission, in March of 1979, the task team critiqued the plans. At that point we were anxious to shift from a planning to an implementing exercise. A substantial majority of agencies submitted plans that were generally adequate. OMB provided them with written critiques and instructions to make revisions correcting the deficiencies cited and begin immediate implementation. For the few agencies that needed additional guidance, OMB scheduled meetings to go over the plans in greater detail. These agencies were given the same instructions: correct and implement at once.

3. Q: "In response to the question on size and technical capability of your staff devoted to security matters, you cited the total number of OIRA staff. Please provide the names and technical backgrounds of those staff members who spend at least 50 percent of their time on computer/communications security."

A: OIRA staff members are responsible for implementing and overseeing provisions of the Brooks Act, the Paperwork Reduction Act, the Privacy Act, and Executive Order 12291. No individual spends more than 50 percent of his or her time on any single aspect of these activities.

4. Q: "You stated that the definition of computer crime was not a problem. How would you define it? What is your assessment of opinions held by others that computer crime is difficult to define?"

A: What I said in testimony was that the definition of computer crime was not a problem, but that there _were_ gray areas exposed by the hackers that may need some _attention_. Generally, there are criminal statutes, either Federal or State, that cover criminal activity involving a computer. Currently, however, there are no Federal and few State statutes that make the mere unauthorized accessing of a data base a crime in itself. This is an area that we need to look at carefully but cautiously.

5. Q: "Should different levels of security be assigned to nonclassified information so that public access is unimpeded for noncritical items but highly controlled for certain critical items? If so, how would you categorize both the information and the protection levels?"

A: I'm not sure that a national system for classifying non-national security information is workable or desirable. With the national security classification system you have a single touchstone for determining level - damage to the security of the nation. With other kinds of data you have many different standards. Integrating them into some kind of overall system would be difficult, perhaps impossible. Instead, what we have right now are a series of _ad hoc_ systems that do the same thing. For example:

- Implicit in the exemption provisions of the Freedom of Information Act is the idea that there is some information that is sensitive enough that the government has a right to withhold it.

- The Privacy Act of 1974 makes sensitive information about individuals subject to certain protections.

- The Internal Revenue Code does the same thing for tax information.

There are many others: the Trade Secrets Act, the Electronic Funds Transfer Act, the Census Act, to name a few. Each statute typically has penalties for misuse that are generally related to the sensitivity or some other rational measure of the data to be protected. This approach, it seems to me, makes more sense than attempting to fit everything into an overall integrated scheme.

6. Q: "In the September 12, 1983 Federal Register, OMB announced plans to develop a new circular for Federal information management based on four existing circulars. Why is OMB excluding applicable provisions of Circular A-123, 'Internal Control Systems'? Do you believe that information security goals are a subset of the overall internal controls used by management to preserve the integrity of agency operations?"

A: The review process that triggered our review of these circulars charged us with reviewing just the four cited. Comments we are receiving in response to our Federal Register notice have raised the issue of including A-123 in this review, and we are considering this possibility. The vulnerability assessments Circular No. A-123 requires, however, cover a much broader area than computer security. In any case, the revised integrated information policy circular that emerges will contain many of the elements of Circular A-123 pertaining to computer security. If A-123 remains as an independent circular, it and our new circular will be consistent and reinforcing.

7. Q: "Although OMB Circular A-71, Transmittal Memorandum No. 1, requires agencies to make risk analyses for data processing systems, it does not specifically require such analyses for data telecommunications networks. How do you ensure, therefore, that agencies implement total systems of controls over all components of their systems, including networks? Describe any plans you have to provide specific guidance on telecommunications."

A: Let me reemphasize a point I made in my statement: when we issued TM No. 1 to OMB Circular No. A-71, it was during a time when everyone's focus was on making the computer center itself secure. Networking was at a very elemental stage. That is not the case now, and telecommunications security is certainly one of the areas we will address in our rewrite of our information policy circulars.

8. Q: "Why has OMB failed to respond to GAO'S Report, 'Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive and Illegal Practices' (MSAD-82-18, April 21, 1982)? Does OMB plan to respond? If so, when?"

A: We think our September 12, 1983 announcement of our plans to develop a new Circular for federal information management responds to many of the GAO findings in the report cited. GAO appears to share this view. In their testimony before your committee, they cited this development as a promising sign of OMB interest in this area and a de facto response to their major recommendation in the report that OMB revise TM No. 1 to OMB Circular A-71.

Mr. Glickman. How do you monitor compliance to the Transmittal No. 1, you know, the statement that requires each agency to do the things that are contained in that circular?

Mr. Wright. ORA continually does reviews over the agency programs and ADP and computer security and then we also do this on an annual basis through our budget reviews. We will be paying a little bit more attention to that this year because, like I said before, we are doing full management reviews for the first time. But for the most part, we rely upon the agencies and the management of the agencies to make sure that they are properly adhering to Transmittal Memo No. 1.

The interesting thing this year, for the first time, and that is the Financial Management Integrity Act that the Congress passed, is going to require the vulnerability assessments and by the nature of that act and the reporting requirements, they will be getting into computer security because, from the standpoint of vulnerability, many of these agencies, like John mentioned, whether it be the Social Security or the IRS, that is a potential real area of vulnerability for the agencies.

Mr. Glickman. We talked a little bit about your resources to monitor compliance with current computer security policy. Do you think you have the technical manpower resources to do the job?

Mr. Wright. I think we have the technical resources to do the job reasonably well. No; I believe that we've got to upgrade our resources in light of the advancements that are being made, particularly in the micro area and the telecommunications area.

Mr. Glickman. And are you doing that?

Mr. Wright. We are in the process of doing that right now. We decided that it was important enough this year not to just begin hiring people, so we brought in the technical resources from the other agencies, primarily GSA and National Bureau of Standards.

Mr. Glickman. You talked about this vast amount of computers, 12 billion dollars worth, 25,000 mid- and large-sized computers, 250,000 to 500,000 microcomputers. We have several new computers that are coming onboard that are just going to almost—one alone is going to double that, and that's the FAA's computer modernization effort. I notice the FAA had the largest telephone bill in the Government, and I assume—at least the Department of Transportation did—I assume that was largely because of the FAA's operations.

Is it reasonable to assume that the threat of computerized resources may also increase with what I see as a large general increase in the number of computers coming onboard?

Mr. Wright. You mean the threat to the security——

Mr. Glickman. Uh-huh.

Mr. Wright [continuing]. Will increase because of the number? No. I—that could happen, but I'm not as concerned about that as probably I would have been 5 or 6 years ago, because you also have many of the machines and the systems that are coming in with fairly sophisticated built-in security devices.

I also believe that we do have the policies and we do have—the guidelines are out there even though they have to be upgraded in the areas I mentioned, so I don't see that as an overwhelming problem right now.

I guess the thing that I would say is we have to make sure that, first of all, the policies and the guidelines are very clear throughout all agencies and that the managers know that this is a major part of their responsibility, not just the effective operation of that ADP center, but also the effective security of it.

Mr. GLICKMAN. Well, I would just tell you this, that in the last day of hearings, we had the folks from Los Alamos Laboratory there and they testified as to the nature of their security operations and how their computers were accessed and invaded and while they were—they protested very strongly that nothing secure was really damaged—and it may not have been—I judged them to be quite defensive as well as—I should say not having the focus on the computer security side of the picture that they might have had and I don't detect that they are any different, probably, than the operators of any computers. That is, particularly in the Government.

They just never thought that this kind of thing would happen. They didn't change their access code like they should have. They did not do the kinds of things and that—the sloppiness which may have been there was—is—could exist everywhere in the Government, even in the Social Security Administration. And even if the FDIC, even in the Federal Reserve System—and you just talk about the fact how our lives are affected, and you've talked about several things in your statement that will try to beef up the computer security in the Government, and I would just urge you to really give this high-priority attention because I think the money and lives and privacy of millions of Americans are affected by this.

Mr. WRIGHT. I agree with you, Mr. Chairman, entirely. I think that the hearings that you're holding right now are pretty timely, not just, you know, because we wouldn't be taking some action anyway in light of all the attentions that's being caused, but it's also one in which we're going through a real evolution of computer and telecommunications technology, and whenever you do that, you're going to have the potential for fraud and abuse in it.

Mr. GLICKMAN. Do you—I mentioned this before—do you have good technical people? What kind of technical staff do you have or do you rely on OSTP or a variety of maybe DOD people? Does OMB have technical people, telecommunications, computer security, scientific people who understand the changing evolution in science?

Mr. WRIGHT. OK. As I mentioned before, Mr. Chairman, yes, we do have people that—within OMB—that are technically capable, but like I also say, I think we have to upgrade this. We have to beef it up a little bit. We do use the ICSt organization from Standards and GSA and Defense and they have brought in a fairly large number of people to work with us on the management reviews that we're going through exactly at this time. But while we do have some very qualified individuals, we still probably should beef that up.

Mr. GLICKMAN. Do you see opportunities for Federal agencies to assist the private sector in its need for computer and communications security?

Mr. WRIGHT. Sure. I think we can probably be very helpful and I believe you've got a couple of agencies that are going to be coming in, you know, after me. Is NBS coming in and—OK, and they can probably answer that better than I can.

Mr. GLICKMAN. And let me ask you this, has a system for classifying nonnational security data according to the need for protecting it ever been considered? Such systems are used in the private sector quite a bit.

Mr. WRIGHT. Nonnational security?

Mr. GLICKMAN. Uh-huh.

Mr. WRIGHT. I don't believe that that issue has ever been seriously looked at to my knowledge. I think that's something that we could probably——

Mr. GLICKMAN. But you haven't considered it——

Mr. WRIGHT [continuing]. Consider——

Mr. GLICKMAN [continuing]. As of this time?

Mr. WRIGHT. No, sir.

Mr. GLICKMAN. OK.

I mentioned in my opening statement, there has been a split between civilian and defense computers. The ARPAnet, it's called, DOD. Were you involved at all in that?

Mr. WRIGHT. John.

No, we were not.

Mr. GLICKMAN. Should you be involved in some of this?

Mr. WRIGHT. From an overall review standpoint, I think it's a good idea because of the fact we can use that experience and use it across agency lines which can be a very useful function that OMB plays. As far as I know, I think that that was a very intelligent thing to do in terms of breaking out your operating from your scientific, you know, ADP functions, and we're going to be looking at that as to application across the various agencies.

Mr. GLICKMAN. OK. Well, I would thank you for coming here. I would say that one of the things that strikes me is that in this highly changing area, that you need to make sure that your own role is clarified. It looks to me like if anybody is managing the problem from a Federal perspective, it's OMB——

Mr. WRIGHT. Uh-huh.

Mr. GLICKMAN [continuing]. Although, as you point out, you are not getting into a lot of the nitty-gritty aspects of the computer security problem and I would dare to say that a lot of Federal agencies at this stage need to be helped and guided along rather dramatically and so I would urge you to highlight this problem.

Mr. WRIGHT. Mr. Chairman, I fully agree with you and as you and I both know, there's all types of helps and guidance and in this area, particularly where you have Inspector Generals coming out and saying that you've got two things: No. 1, you've got a certain lack of information that's out there, despite the fact that it's right in circulars that are available; and also perhaps a certain lack of appreciation that computer security is a problem, potential problem, and that it is the responsibility of the individual managers to make sure that they put that high on their list of priorities and that is something that we can do very well—

Mr. GLICKMAN. OK——

Mr. WRIGHT [continuing]. And we will do that.

Mr. GLICKMAN. Thank you very much for being here.

Our next witness is Warren Reed, Director of Information Management and Technology Division, U.S. General Accounting Office.

Mr. **Reed**. Good morning.

Mr. **Glickman**. Mr. Reed, it's a pleasure to have you here this morning. As I mentioned to our last witness, and all witnesses here, your entire statements will appear in the record so you may feel free to summarize if you wish.

STATEMENT OF WARREN REED, DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, U.S. GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY WALTER L. ANDERSON, SENIOR ASSOCIATE DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION; AND HAROLD J. PODELL, GROUP DIRECTOR WITH INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

Mr. **Reed**. Thank you very much. I would like to do that. I have with me Dr. Harold Podell and Mr. Wally Anderson from my staff.

Our basic message today, Mr. Chairman, is that vulnerabilities and threats in this general area are on the rise and will continue and I think our testimony will—or written statement will—provide ample evidence of that.

There are legislation policies, management and internal audits that can provide a framework for counteracting the increasing vulnerabilities. However, our findings over the years demonstrate quite convincingly, we believe, that each area has inherent weaknesses. Agencies need to devote more management attention and resources to implementing total systems of controls.

On a more positive note, Government-wide and agency-specific initiatives currently underway appear to be fostering this goal. Our assessment of these initiatives is the best one of cautious optimism and I'll amplify on that general message.

I think the general threats can be—that we have to contend with can be categorized as natural hazards, unintentional actions, and intentional actions. And, of course, the latter, intentional actions, receive considerable attention. They include attacks on equipment, improper access to and disclosure of information which should be held private and so on.

A variety of technical methods can be used to penetrate computer systems for these purposes. The spread of microcomputers provides potential penetrators with increased opportunities to access and manipulate data bases.

In spite of the sophistications and complexities of the hardware/software and communications networks, we believe that information security is basically and principally a management problem, not a technology problem, and requires a concerted management solution.

Let me offer at this point some observations from approximately 40 reports that GAO has issued since 1976 related to information security. I will not belabor the findings, but I will just give you the essence. I think they are addressed somewhat thoroughly in my written statement.

In the area of legislation we found the need for at least one revision related to legalities of wiretapping using electronic devices. In the area of policy, that we were talking about—or addressing with the previous witness, we found major deficiencies in OMB's principal guidance document for information security, circular A-71, Transmittal Memorandum No. 1, the one that focuses on information security.

With the respect to management initiatives, we reported that key central agencies—OMB, GSA, NBS, OPM—have provided incomplete and uncoordinated guidance and have not insured that agencies complied with existing guidance. We also reported that executive agencies were not doing enough to implement information security program policies and guidance.

Finally, in the area of audit activity, we reported at least three major areas in which Federal audit units had not met their audit responsibilities of automated systems. I should add what I have just reported to you is a historical perspective. On a more positive note, our written statement describes a number of current initiatives that may become vehicles for enhancing information security. Let me touch on some of these.

First, 18 agencies responded favorably to our April 1982 audit entitled, "Federal information systems remain highly vulnerable to fraudulent, wasteful abuse of an illegal practices." All agencies indicated they are taking or plan to take constructive actions. I might add OMB did not respond to that audit.

Second, OMB plans to revise existing circulars on information management, and that is one I think the previous witness was alluding to. As he indicated, in a September 12, 1983, Federal Register notice, OMB announced plans to develop a new policy circular on Federal information management. The proposed circular would consolidate four existing circulars, including those on information security.

Third, the Financial Integrity Act, also mentioned earlier, may foster the development of information security control. And I concur with the previous witness, this is a very important effort. This act requires that agencies evaluate internal controls and that they annually report the results of their evaluations to the Congress and the President.

The act also requires that internal controls provide reasonable assurance that assets are safeguarded against waste loss, et cetera. It thus places the administrative, physical and technical controls used to provide information securities squarely within the context of the agency's overall system of internal controls. If agencies perceive this clear link between the security controls and overall management controls, we should have a mechanism for security measures to receive renewed emphasis.

Fourth, DOD information security techniques and knowledge could be shared. On January 2, 1981, DOD formed the DOD Computer Security Center. The general mission of this center is to provide technical support for computer security, evaluate commercial software and hardware systems, conduct and sponsor research in computer and network technology, and disseminate computer security information.

The center could be very useful for civil agencies to use in conducting computer and communications risk analyses in employing other techniques.

I would now like to close, Mr. Chairman, by offering the following observations.

In the policy area of the OMB action to develop a policy circular for Federal information management is a positive step and is long overdue. We are not expecting a cookbook of absolutes here, but we do believe a comprehensive policy is needed.

We are concerned that we don't see more direct evidence here by OMB to incorporate provisions of Circular A-123 on internal control systems into its expanded information management circular. As mentioned, this circular or the Circular A-123 provides internal control policy guidance for agencies to use in implementing the Federal Manager's Financial Integrity Act of 1982.

This internal control policy and computer security policy, as represented in Transmittal Memorandum No. 1, both serve to—both serve to safeguard agency assets from waste, loss and abuse and should be considered essential tools for information resources management and should be considered together.

Recent management actions by the central agencies are very encouraging. One of the more formidable challenges will be effective followup by OMB, as Mr. Wright alluded earlier in reviewing agency compliance with policy initiatives.

Executive agency action is the most critical factor in terms of its capability to have a tangible and timely impact on security. Agency followthrough on plans for sharpening focus on information security can be a major advance.

Likewise, if the agency evaluations of internal controls in response to the Financial Integrity Act before the appropriate attention to information security, the threats alluded to earlier should be minimized. If these evaluations do not address information security controls, however, a critical opportunity will be lost or, at best, deferred.

Finally, I would like to make it clear this—my remarks today and our—and my written testimony are not intended to represent a complete inventory of the existing potential information problems or solutions.

For example, faithful efforts by OMB to review the agency's information resources management activities every 3 years, as required by the Paperwork Reduction Act, could have a positive impact. Moreover, recent reports of the President's private sector survey on cost control, or the Grace Committee, call for stronger governmentwide emphasis on information resources management.

The committee called for OMB to exercise more aggressive management leadership. Also, the administration's reform 1988 program has set a goal of making Federal computer and communications systems more compatible, so that waste, fraud and abuse of programs can be reduced.

Now, GAO will be closely monitoring all of these activities. Currently, we are reviewing agency's implementation of the Financial Integrity Act. As part of this effort, we will be looking closely at the agency's vulnerability assessments, including those of automated systems and the degree to which they address information security.

In closing, we welcome all the positive steps taken to date. We must await, however, more tangible evidence of results to determine if the rate of progress is keeping pace with the increasing threats.

This completes my remarks. I would be glad to address any questions.

[The prepared statement of Mr. Reed follows:]

B

U. S. GENERAL ACCOUNTING OFFICE

WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 A.M., EST
MONDAY, OCTOBER 17, 1983

STATEMENT OF

WARREN G. REED

DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS
COMMITTEE ON SCIENCE & TECHNOLOGY

HOUSE OF REPRESENTATIVES

ON

TELECOMMUNICATIONS SECURITY AND PRIVACY

Mr. Chairman and Members of the Subcommittee:

We are here today at your request to discuss telecommunications and related computer security and privacy issues. Our testimony is based on the knowledge of the subject we gained in numerous audits of federal government executive departments and agencies over the past several years.

In this testimony I will discuss the information security environment from four different standpoints. First, I will discuss the nature of the information security problem today as it affects our automated systems and, increasingly, their supporting telecommunications networks. I will describe the different types of threats we must protect our systems against and indicate the reasons why the problem is growing more serious. Second, I will describe the key factors of legislation, policy, management, and auditing which affect information security. Third, I will summarize our audit findings over the past 7 years in relation to these key factors and indicate shortfalls which have contributed to security problems. Finally, I will discuss recent federal initiatives that, collectively, could have an important impact on solving these problems.

Our basic message is that the vulnerabilities facing our computer systems and telecommunications networks are increasing as technology advances. The growing numbers of remote computer terminals which provide access to very large data bases make errors or deliberate attacks difficult to discover and fix. Legislation, policies, management roles, and audits provide a framework for counteracting these vulnerabilities but further steps are needed. In particular, agencies need to devote more management attention and resources to implementing total systems of control. Government-wide and agency-specific activities underway appear to be fostering this goal.

THE NATURE OF THE INFORMATION SECURITY PROBLEM

The federal government depends heavily on computers and telecommunications networks today to handle information on functions ranging from defense and intelligence to banking and financial activities, health, and education. Much of this information is personal, proprietary, or otherwise sensitive and requires effective security. Information security has three basic components: computer security, telecommunications security, and supporting systems security.

GAO reports since 1976 and examinations by others have repeatedly demonstrated that federal information systems are subject to three broad categories of threat: (a) natural hazards,

(b) unintentional actions, and (c) intentional actions. Natural hazards include fire, floods, earthquakes, etc., that can damage or totally destroy equipment, software, and data or seriously interrup operations through extended power outages. Unintentional actions include equipment failures and malfunctions and improper design of systems failures as well as personnel errors and inappropriate actions. The latter two pose the more serious threats. Intentional actions, which receive considerable attention, include attacks on equipment, improper access to and disclosure of information which should be held private, and unauthorized alteration of official records. A variety of technical methods can be used to penetrate computer systems for these purposes.

Providing a reasonable level of protection in today's technological environment is a formidable challenge because the range of vulnerabilities is increasing. The larger systems in use can store more sensitive information in electronic form. The expanded use of remote terminals provides more isolated points of access and makes it difficult to pinpoint errors or attacks. Similarly, the advent of microcomputers provides more individuals with the potential capability to access, create, and manipulate data bases by bypassing central controls. The trend toward linking computers and terminals through telecommunications networks provides potential penetrators with more opportunities, techniques, and devices to access systems, to insert communications, and to intercept and interpret communications.

In spite of the sophistication and complexities of our hardware, software, and communications networks, we must keep in mind that information security is basically a management problem, not a technology problem, and requires a concerted management solution.

KEY FACTORS AFFECTING INFORMATION SECURITY

Legislation, policy, management by central and executive agencies, and auditing are the key factors that support Federal efforts to provide security.

Legislation

Legislation serves to define information security goals and objectives and to assign overall management responsibilities for security. A variety of laws have been enacted governing different security activities.

The Brooks Act of 1965 (Public Law 89-306), which amended the Federal Property and Administrative Services Act of 1949, assigned the Office of Management and Budget (OMB), the General Services Administration (GSA), and the Department of Commerce collective responsibility for managing agencies' acquisition and maintenance of ADP resources, but placed OMB in a leadership role. The Federal Communications Act of 1934, as later modified by the Omnibus Crime Control and Safe Streets Act of 1968 (Public Law 90-351), provided for the protection of electronic transmissions. The Privacy Act of 1974 (Public Law 93-579) prescribed controls over personal records dissemination and access. The Paperwork Reduction Act of 1980 (Public Law 96-511) broadened OMB's responsibilities in the context of information resources management. Finally, the Federal Managers' Financial Integrity Act of 1982 (Public Law 97-255) directed evaluations of administrative and financial internal control systems and agency accounting systems. It further required annual reports on these systems. In 1983 GAO published standards for Internal Controls in the federal government to be used by agencies to establish and maintain effective systems of internal control in compliance with the act.

Policy

Information security policy should provide agencies with a clear and concise blueprint for implementation of relevant legislation. It should faithfully reflect legislative intent, completely address all pertinent features of the legislation, and be compatible with other related policies.

OMB is the key policymaker in this area. Circular A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Systems," issued July 27, 1978, outlines basic policy and specifies agencies' responsibilities for the development and implementation of security. In particular it assigns government-wide responsibilities to GSA, Commerce, and the Office of Personnel Management (OPM). OMB Circular A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," issued July 1, 1975, requires agencies to establish reasonable safeguards against improper disclosure of such records. OMB Circular A-123, "Internal Control Systems," revised August 16, 1983, after passage of the Financial Integrity Act, prescribes policies and guidance for establishing and maintaining internal controls over program and administrative activities. It mandates that all levels of agency management help assure the adequacy of these controls.

Management

Management responsibilities are divided among four "central agencies" (OMB, GSA, Commerce, and OPM) and the remaining executive agencies.

The central agencies should issue policies, guidelines, and regulations that are consistent and coordinated with each other and contain "how-to" specifics where applicable to assist executive agencies in meeting legislative and Executive Office requirements. They also should oversee agencies' implementation of their guidance.

The central agencies have related yet separate responsibilities. OMB must review agencies' organizational structures and management procedures to ensure they meet policy requirements. GSA is required to issue policies and regulations for the physical security of computer rooms and to ensure that agency procurement requests for computers include appropriate security requirements. The Department of Commerce is responsible for developing uniform federal ADP standards including security standards. It has delegated this responsibility to the National Bureau of Standards (NBS). OPM is responsible for establishing personnel security policies for federal personnel associated with the design, operation, or maintenance of computer systems or having access to data in these systems.

The executive agencies play the most vital role in protecting our information assets. They must develop and implement agency information security programs through a set of policies and procedures which conform to the requirements of applicable legislation and guidance. Their security programs should provide a reasonable, yet cost-effective, level of protection. Agency management should base their programs on assessments of risk and ensure that they incorporate administrative, physical, as well as technical controls. Finally, agency management must monitor the implementation of their programs.

Agency managers employ a wide variety of techniques to achieve a total system of control. A technique known as risk analysis is used to ascertain the extent to which information systems are vulnerable to natural disaster, human error, and improper or illegal use. This provides a basis for a program to minimize the effects of such vulnerability. Other related techniques include background investigations for employees and contractors associated with computers; contingency plans for emergency response in the event of system failure; backup and recovery capabilities to keep systems operating in the wake of disaster; and the use of encryption devices to protect personal data transmissions.

Audits

Systematic internal audits provide management with periodic reports on the level of protection actually provided over automated systems and particularly their sensitive applications. Management can use these reports to identify needed corrective measures.

OMB Circular A-71, Transmittal Memorandum No. 1, requires agencies to conduct periodic audits of security safeguards. It specifies that these audits be performed by an organization independent of the user organization and computer facility managers.

The Comptroller General has issued specific standards for auditing programs supported by computer-based systems. These standards prescribe that auditors review both general systems and applications controls. They also suggest that reviews be conducted during the early stages of system design and development. Circular A-123 requires that agencies provide for ongoing internal control reviews and that agency inspectors general assist in this process.

GAO AUDIT FINDINGS
RELATED TO KEY FACTORS

Since April 1976 GAO has issued about 40 reports related to information security. These reports have identified deficiencies in several areas including the following (numbers are approximate):

--Legislation (1).

--Policy (10).

--Management (15).

  Central agency and executive agency management (7).

  Internal controls (8).

--Internal audit (3).

Many issues have been reported on repeatedly during this period. For example, the first GAO report on the implementation of Circular A-71, Transmittal Memorandum No. 1, was issued in 1979 and at least six other reports addressed this issue in 1979, 1980, 1982, and 1983. We have not comprehensively updated our major security findings since 1982; however, we have performed work at selected agencies. I will highlight our findings bearing directly on information security.

Legislation

Our review of applicable telecommunications security legislation showed that the Communications Act of 1934 and the Crime Control Act of 1968 are inadequate with respect to interceptions of wire communications, or "wiretapping." The 1934 Communications Act did not define the term "interception." The Crime Control Act of 1968, as amended, used the qualifying term "aural acquisition" (acquired by use of the ear) to define interception. As a result, only interceptions by aural means are illegal under this act, unless authorized by court order. Therefore, we conclude that as long as the term "aural" remains as a semantic qualifier in the 1968 Crime Control Act's definition of interception, anyone can conduct unauthorized nonaural wiretapping of data telecommunications without a court order and not be in violation of this law.

The definition of interception under the Crime Control Act of 1968 is conceptually different from the definition of "electronic surveillance" in the Foreign Intelligence Surveillance Act of 1978, Section 1801 of Title 50, United States Code, which by definition is not limited to "aural" interception.

Policy

We reported that OMB Circular A-71, Transmittal Memorandum No. 1, the primary Federal guidance for information security, needed revision, in part, to:

- --Identify the minimum controls necessary to ensure a reasonable level of protection over personal, proprietary, and other sensitive information.
- --Clarify when executive agencies must afford the same level of protection for such sensitive information as they do for information classified for purposes of national security.

--Establish policy and specific guidance for protecting systems using telecommunications networks.

Management

We have reported that the central agencies had provided incomplete and uncoordinated guidance and had not ensured that agencies complied with existing guidance.

OMB issued pertinent circulars such as Circular A-71, Transmittal Memorandum No. 1, and Circular A-123 on internal controls. However, it had not taken adequate action to ensure that executive agencies were effectively implementing their information security programs in compliance with Circular A-71, Transmittal Memorandum No. 1 which we stated should be revised.

GSA had not adequately cross-referenced the Federal Property Management Regulations (FPMRs) on ADP and telecommunications with the applicable NBS Federal Information Processing Standards Publications (FIPS PUBS) on security.

NBS planned to issue 36 standards it considered necessary to achieve a reasonable level of protection over executive agencies' automated information systems. However, we reported in 1982 that NBS had issued only six guidelines and one standard addressing various aspects of security.

OPM's guidance for personnel security needed strengthening. For example, the "grandfather" provision in OPM's Federal Personnel Management Letter 732-7 permitted many experienced employees to receive security approvals without a background investigation appropriate to the sensitivity of their positions.

Regarding executive agency management, we reported that the executive agencies were doing little to implement information security program policies and guidance. Further, we reported that some senior managers were not fully aware of how highly vulnerable their systems are to fraudulent, wasteful, abusive, and illegal practices. For example, in September 1983 we reported that the Arms Control and Disarmament Agency had not developed an information security program, had not performed required risk analyses, and had not conducted required security audits. As a result, management could not be sure computerized information was adequately protected. A key computer services official believed the potential existed for loss of valuable data.

We found that most executive agencies generally selected, implemented, and maintained a system of controls based on personal insight rather than on the use of risk analysis techniques. Risk analysis techniques provide a sound basis for management to implement and maintain a total system of controls which balances the costs of protection against the risks posed by fraudulent, wasteful, abusive, and illegal activities and natural disasters. The most cost-effective time to incorporate such controls into a system is when it is being designed.

Required personnel background investigations were not always performed. For example, we reported that the security officers at two agencies did not have extensive background investigations completed for themselves, even though both occupied positions defined by OPM as being highly sensitive. The omissions occurred because the agencies that employed them had not defined their positions in accordance with OPM guidance.

Audits

We reported at least three major areas in which Federal internal audit units had not met their automated information system responsibilities.

First, we found that several internal audit organizations had not provided adequate audit coverage for their agencies' computer systems and applications. One reason was that, although Circular A-71, Transmittal Memorandum No. 1, required such audits, it did not specifically assign them to the internal audit function.

Second, we reported that internal auditors did not always comply with Comptroller General audit standards for reviewing computer-based systems.

Third, we reported that many audit organizations had not developed or maintained appropriately skilled audit staff. Staffing was hindered by lack of management support, personnel ceilings, and hiring restrictions. We identified the need for formal training programs for automated information system auditing.

We believe this synopsis of GAO's audit findings of the past few years provides ample evidence that serious shortfalls exist in each factor relating to information security. We have found policy gaps, serious management deficiencies at both the central and executive agency level, inadequate internal audit capabilities, and at least one needed revision to law. Because of these shortfalls, information system losses continue to occur due to accidental and intentional causes. For example, we reported that in April 1982 the U.S. Attorney's Office in Los Angeles successfully prosecuted a Social Security Administration field office employee who had fraudulently used the telecommunications network to steal more than $104,000 in supplemental security income benefits. This was the third such case prosecuted by that office since 1980. We also reported that in 1981 the military services overpaid military retirees and survivors about $5 million because the Veterans Administration did not inform the services that it had paid compensation to these individuals. The Veterans Administration's failure to inform the services through its automated information system was due to a combination of (1) clericial oversight or error in not reporting award data and (2) incomplete records that did not indicate the award recipient was a military retiree or survivor.

CURRENT ACTIVITIES TO IMPROVE SECURITY

To place the above findings in perspective, we have attempted to identify current initiatives in each of the four categories of supporting factors that may become vehicles for enhancing security.

Legislation

Proposed legislation addresses computer crime

Identical bills were introduced in the House and Senate this year which would establish criminal penalties for fraudulent or illegal use of computers owned by, operated by, or under contract to the U.S. Government. H.R. 1092 and S. 1733, "The Federal Computer Systems Protection Act," stem from the recognition that, although computer or information system crimes can cause substantial financial loss, they have been difficult to prosecute under existing laws. If passed, the legislation could potentially help the government take punitive action against those who intentionally misuse its automated systems.

Policy

OMB plans to revise existing circulars on information management

In a September 12, 1983, Federal Register notice, OMB announced plans to develop a new policy circular on federal information management. The proposed circular would consolidate four existing circulars, including Circular A-71, Transmittal Memorandum No. 1, on information security and Circular A-108 on the maintenance of records about individuals. OMB is considering framing the circular to address a wide range of issues which go beyond the scope of current policy. One such issue is the security implications of the new environment of end user computing, which can involve telecommunications networks and microcomputers.

Thus, although OMB did not respond to our April 1982 recommendation that it revise Circular A-71, Transmittal Memorandum No. 1, its plans for a comprehensive information policy indicate that it may recognize the need for improvements in these areas.

Management

Numerous agencies have responded to our April 21, 1982, audit

On April 21, 1982, we made major security-related recommendations to OMB, GSA, NBS, and OPM and to the heads of the other executive departments and agencies in our report, "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices." We received responses from 18 agencies, with the major exception of OMB. In January of this year, GSA updated the FPMRs as we had recommended to provide a current cross-reference to the NBS FIPS PUBS on security and related documents. The eighteen agencies generally responded that they shared our security concerns and agreed with our recommendations that agencies conduct risk analyses, incorporate them into new information security programs, and institute internal audits of the programs' implementation. The majority stated they have either taken or planned related action.

Three of the eighteen agencies objected to our major recommendation that OMB revise Circular A-71, Transmittal Memorandum No. 1, to provide more specific guidance on needed controls and on vulnerability assessments of telecommunications networks. Their concerns focused, in part, on the potential for overcentralization if a revised circular required extensive OMB involvement in the agencies' development and operation of automated information systems.

The central agencies are focusing more attention on information security

The central management agencies are more actively addressing the need for effective federal information security. I mentioned the OMB announcement to revise certain circulars, including Circular A-71, Transmittal Memorandum No. 1, and the update of the FPMRs by GSA. GSA has also issued a temporary FPMR that consolidates government-wide management guidance regarding both automated data processing and word processing technologies. OPM has informed us it will evaluate the issues we raised in our April [illegible] report, including the waiver of investigations for certain employees. Finally, NBS has issued and is developing additional FIPS PUBS guidance on information security.

The Financial Integrity Act will foster the development of information security controls

As mentioned, the Financial Integrity Act requires that agencies evaluate internal accounting and administrative controls and that they annually report the results of their evaluations to the Congress and the President. These agency evaluations must consider the Comptroller General's internal control standards published in 1983.

The Act also requires that internal controls provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. It thus places the administrative, physical, and technical controls used to provide information security squarely within the context of the overall system of agency management's internal controls. The act makes clear the link between the security and management functions and provides a mechanism for security measures to receive renewed emphasis.

DOD information security techniques knowledge could be shared

The Department of Defense (DOD) has been a pioneer in computer and communications security technology for many years and therefore has a wealth of knowledge that could be of benefit to the civil agencies. Let me give a brief background on our work related to the DOD Computer Security Center.

We recommended in an April 5, 1978, report, "Multi-Level Computer Security Requirements of the World Wide Military Command and Control System," that DOD consolidate many of its research and development activities on computer security. On January 2, 1981, DOD formed the DOD Computer Security Center as a first step in complying with our recommendation. The Center could be a useful resource for civil agencies to consult when conducting computer and communications risk analyses and employing other techniques.

Audits

The President's Council on Integrity and Efficiency is emphasizing audit activities

The President's Council on Integrity and Efficiency, established in March 1981, is taking steps that may improve information security in the federal agencies. The council, chaired by the Deputy Director of OMB, and composed of the Deputy Attorney General, the Director of OPM, and the Federal Bureau of Investigations Executive Assistant Director of Investigations, inspectors general, and other agency designees, is focusing on:

--Standards for the management, operation, and conduct of inspectors general and similar operations in all agencies.

--Efforts to develop a corps of well-trained and highly skilled auditors and investigators.

- --Comprehensive plans for government-wide activities attacking fraud and waste.
- --Joint projects involving many agencies in special audits and investigations.

An example of the Council's activities in information security is the June 1983 report, "Computer Related Fraud and Abuse in Government Agencies." The report was prepared for the Council by an interagency committee of inspectors general.

SUMMARY

We have attempted in this testimony to underscore the serious nature of computer and telecommunications security vulnerabilities. The potential for loss is increasing because we are concentrating more information--a valuable resource--in automated systems. Also, potential penetrators will have easier access to automated systems using microcomputers, a technology whose sophistication is a long way from peaking.

We have also attempted to provide a balanced perspective on both the information security problems and the potential solutions underway. We wish to emphasize that all agencies have a substantial stake in security and all must contribute to achieving it.

In the policy area, the OMB action to develop a policy circular for federal information management is a positive step and is long overdue. We are not expecting a "cookbook" of absolutes but we do believe a comprehensive policy is needed. It remains problematic what line, if any, should be drawn, between internal control policy and computer security policy; both serve the objective of safeguarding funds, property, and other assets from waste, loss, and unauthorized use.

Recent management actions by the central agencies are encouraging. One of the more formidable challenges will be effective follow-up by OMB in reviewing agency compliance with policy initiatives, particularly those associated with the Financial Integrity Act on internal controls. Equally challenging for the central agencies will be fostering an environment where exchange of information on security techniques between civil and defense sectors can be accomplished.

Although strengthened legislation and policy can serve as aid to improving information security, executive agency action is the most critical factor in terms of its capability to have tangible and timely impact. Agency follow-through on plans for sharpening focus on information security will be a major advance. Likewise, if the agency evaluations of internal controls in response to the Financial Integrity Act afford the appropriate attention to information security, all threats alluded to earlier should be minimized. If these evaluations do not address information security controls, however, a crucial opportunity will be lost or, at best, deferred.

The combined impetus provided by the President's Council on Integrity and Efficiency and the inspectors general should bolster internal audit capabilities.

—— —— —— ——

This testimony is not intended to be a complete inventory of the existing or potential information security problems nor does it account for all the progress that is underway. Other developments include OMB efforts to review the agencies' information resources management activities every 3 years as required by the Paperwork Reduction Act. Also, the recent reports of the President's Private Sector Survey on Cost Control, or Grace Committee, called for a stronger government-wide emphasis on information resources management. The Committee called for OMB to exercise more aggressive management leadership. Finally, the administration's Reform 88 program has set a goal of making Federal computer and communications systems more compatible so that waste, fraud, and abuse of programs can be reduced.

To summarize, legislation, policy formulation by the central agencies, and implementation by the executive agencies are key factors in establishing and maintaining a government-wide information security program. Each plays a unique role yet, to be fully effective, they must function as an integrated system.

GAO will be closely monitoring the activities discussed. Currently we are reviewing agencies implementation of the Financial Integrity Act. As part of this effort we will be looking at agencies' vulnerability assessments including those of automated systems.

We welcome all the positive steps taken to date. We must await more tangible evidence of results, however, to determine if the rate of progress is keeping pace with the increasing threats. This completes my prepared remarks. We would be pleased to answer any questions.

SELECTED GAO REPORTS FROM 1976 TO SEPTEMBER 1983 INVOLVING INFORMATION SECURITY OR FEDERAL COMPUTER MATCHING EFFORTS

The two lists in this attachment contain 1) a representative set of 42 GAO reports on major information security issues and 2) 19 representative reports involving federal computer matching efforts. It should be noted that these are not complete listings, since these topics are discussed to some extent in other GAO reports.

REPORTS INVOLVING INFORMATION SECURITY

1. "Need for Internal Control Improvements at ACDA, Including Adequate Internal Audit Coverage" (GAO/NSIAD-83-68, September 30, 1983).
2. "Need to Improve Management of ACDS's Automatic Data Processing and Operations " (GAO/NSIAD-83-66, September 30, 1983).
3. "Computer Technology at IRS: Present and Planned" (GAO/GGD-83-103, September 1, 1983).
4. "Military Services and VA Can Reduce Benefit Overpayments by Improving Exchange of Pay Data" (GAO/AFMD-83-39, July 12, 1983).
5. "Implementing the Paperwork Reduction Act: Some Progress, But Many Problems Remain" (GAO/GGD-83-35, April 20, 1983).
6. "Inadequate Internal Controls Affect Quality and Reliability of the Civil Service Retirement System's Annual Report" (GAO/AFMD-83-3, October 22, 1982).
7. "Analysis of Internal Control Systems to Ensure the Accuracy, Completeness, and Timeliness of Federal Procurement Data" (GAO/PLRD-82-119 September 23, 1982).
8. "Examination of the Social Security Administration's Systems Modernization Plan" (GAO/HRD-82-83, May 28, 1982).
9. "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices" (MASAD-82-13, April 21, 1982).
10. "The Treasury Department and Its Bureaus Can Better Plan for and Control Computer Resources" (GGD-82-9, February 22, 1982).

11. "Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed" (HRD-82-19, December 10, 1981).

12. "The Bureau of the Census Must Solve ADP Acquisition and Security Problems" (AFMD-82-13, October 21, 1981).

13. "Financial Institution Regulatory Agencies Should Perform Internal Audit Reviews of Their Examination and Supervision Activities" (GGD-82-5, October 19, 1981).

14. "Federal Agencies Still Need to Develop Greater Computer Audit Capabilities" (AFMD-82-7, October 16, 1981).

15. "Financial Control System Problems at the Community Services Administration Will Not Be Fully Solved by the Current System Redesign Project" (AFMD-81-96, August 19, 1981).

16. "Weak Internal Controls Make the Department of Labor and Selected CETA Grantees Vulnerable to Fraud, Waste, and Abuse " (AFMD-81-46, March 27, 1981).

17. "Social Security Needs to Better Plan, Develop, and Implement Its Major ADP Systems Redesign Projects" (HRD-81-47, February 6, 1981).

18. "Disappointing Progress in Improving Systems For Resolving Billions in Audit Findings" (AFMD-81-27, January 23, 1981).

19. "Most Federal Agencies Have Done Little Planning for ADP Disasters" (AFMD-81-16, December 18, 1980).

20. "Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies" (LCD-81-1, November 12, 1980).

21. "Weak Financial Controls Make the Community Services Administration Vulnerable to Fraud and Abuse" (FGMSD-80-73, August 22, 1980).

22. "Central Agencies' Compliance With OMB Circular A-71, Transmittal Memorandum No. 1" (LCD-80-56-I, April 30, 1980).

23. "Flaws in Controls Over the Supplemental Security Income Computerized System Causes Millions in Erroneous Payments" (HRD-79-104, August 9, 1979).

24. "IRS Can Better Plan For and Control Its ADP Resources" (GGD-79-48, June 18, 1979).

25. "Review of DOD's Internal Audits and Policy For Computer Security" (LCD-79-109, March 21, 1979).

26. "Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123, January 23, 1979).

27. "The Bureau of Census' Management and Use of ADP Resources" (FGMSD-79-5, December 13, 1978).

28. "VA's New Computer System Has Potential to Protect Privacy of Individuals Claiming Benefits" (HRD-78-135, July 17, 1978).

29. "Procedures to Safeguard Social Security Beneficiary Records Can and Should Be Improved" (HRD-78-116, June 5, 1978).

30. "Inadequacies in Data Processing Planning in the Department of Commerce" (FGMSD-78-27, May 1, 1978).

31. "Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment" (LCD-76-102, April 28, 1978).

32. "Multi-level Computer Security Requirements of the World Wide Military Command and Control System (WWMCCS)" (LCD-78-106, April 5, 1978).

33. "Privacy Issues and Supplemental Security Income Benefits" (HRD-77-110, November 15, 1977).

34. "New Methods Needed for Checking Payments Made by Computers" (FGMSD-76-82, November 7, 1977).

35. "Computer Auditing in the Executive Departments: Not Enough is Being Done" (FGMSD-77-82, September 28, 1977).

36. "IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information" (GGD-77-44, July 11, 1977).

37. "Vulnerabilities of Telecommunications Systems to Unauthorized Use" (LCD-77-102, March 31, 1977).

38. "Problems Found With Government Acquisition and Use of Computers From November 1965 to December 1976" (FGMSD-77-14, March 15, 1977).

39. "Safeguarding Taxpayer Information--An Evaluation of the Proposed Tax Administration System" (LCD-76-115, January 17, 1977).

40. "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities" (FGMSD-76-40, May 10, 1976).

41. "Computer Related Crimes in Federal Programs" (FGMSD-76-27, April 27, 1976).

42. "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government" (FGMSD-76-5, April 23, 1976).

REPORTS INVOLVING COMPUTER MATCHING

43. "Computer Matches Identify Potential Unemployment Benefit Overpayments" (GAO/GGD-83-99, August 24, 1983).

44. "Statement of W.D. Campbell, before the Subcommittee on Oversight of Government Management, Senate Committee on Governmental Affairs" (December 16, 1982).

45. "States' Capability to Prevent or Detect Multiple Participation in the Food Stamp Program" (CED-82-103, June 16, 1982).

46. "Prisoners Receiving Social Security and Other Federal Retirement, Disability, and Education Benefits" (HRD-82-43, July 22, 1982).

47. "Millions Could Be Saved By Improving Integrity of the Food Stamp Program's Authorization-To-Participate System" (CED-82-34, January 29, 1982).

48. "Legislative and Administrative Changes to Improve Verification of Welfare Recipients Income and Assets Could Save Hundreds of Millions" (HRD-82-9, January 14, 1982).

49. "States' Efforts to Detect Duplicate Public Assistance Payments" (HRD-81-133, September 17, 1981).

50. "Concerns About HHS' Ability to Effectively Implement Incentive Funding for State Information Systems in the Aid to Families With Dependent Children Program" (HRD-81-119, June 29, 1981).

51. "Impact of State Death Information on Federal Income Security Programs" (HRD-81-113, July 28, 1981).

52. "Millions Can be Saved by Identifying Supplemental Security Income Recipients Owning Too Many Assets" (HRD-81-4, February 4, 1981).

53. "VA Improved Pension Program: Some Persons Get More Than They Should and Others Less" (HRD-80-61, August 6, 1980).

54. "Social Security Should Obtain and Use State Data to Verify Benefits for All Its Programs" (HRD-80-4, October 16, 1979).

55. "Social Security Student Benefits for Postsecondary Students Should be Discontinued" (HRD-79-108, August 30, 1979).

56. "Social Security Should Improve Its Collection of Overpayments to Supplemental Security Income Recipients" (HRD-79-21, January 16, 1979).

57. "Duplicate Payments for Student Benefits Under the Social Security Administration's Retirement, Survivors, and Disability Insurance Program" (HRD-79-27, December 22, 1978).

58. "Letter Report on Duplicate AFDC Payments in New York" (HRD-78-133, June 21, 1978).

59. "Wisconsin's Aid to Families With Dependent Children and Child Support Enforcement Programs Could Be Improved" (HRD-78-130, June 22, 1978).

60. "Privacy Issues and Supplemental Security Income Benefits" (HRD-77-110, November 15, 1977).

61. "Supplemental Security Income Payment Errors Can Be Reduced" (HRD-76-159, November 18, 1976).

Mr. **Glickman**. Thank you very much, Mr. Reed.

I want to go back for a moment. You indicated in your statement that the Office of Management and Budget did not respond to the audit recommendations made last year, that 18 agencies did and they did not.

Mr. **Reed**. Yes, sir.

Mr. **Glickman**. Did you ever try to find out why they didn't respond?

Mr. **Reed**. I think we did. I will ask Dr. Podell, who dealt with those responses, to elaborate on the answer.

Mr. **Podell**. I have called the Office of Management and Budget periodically since we issued our report, and my understanding is that they had several draft responses that never could clear OMB. And to this date, we have received no formal response at all in compliance with the law that there should be a response to our recommendations.

Mr. **Glickman**. Well, it is not necessarily unusual that they don't respond, although it is of great concern that this is the chief, so to speak, management body in this Government, responsible for implementing a whole set of changes to try to improve the security problem. And we delegated you the responsibility to indicate what the problems were, and that chief managing body didn't even see fit to respond.

You also indicated in your statement—I would like for you to repeat this again because I couldn't find it in your written statement, I heard you talking about it—some of your concerns regarding the current efforts of OMB. I wonder if you might repeat that to me. I am trying to get a feel of where you believe the Office of Management and Budget is now in connection with their perceived and real responsibilities to try to help Federal agencies deal with this problem.

Mr. **Reed**. Well, yes. I believe one of the most—one of the greatest challenges that OMB has at hand right now is to promulgate a revised policy for information security. The information security policy was issued I believe in 1978 and it was really—that particular policy was an outgrowth or appended to circular A-71, which goes back to an issuance date of 1965, I believe.

The point is, the policy must be updated. OMB understands that. What we are concerned about is that the revised circular that seems to be in the making did not allude, at least in the announcement that we read in the Federal Register, to the incorporation of policy for system controls.

We feel controls are probably the most important mechanism that can be used to better safeguard our information and, therefore, they should be a very principal part of the revised circular that OMB is in the process of issuing.

Mr. **Glickman**. What did they emphasize in their circular if they didn't emphasize system controls?

Mr. **Reed**. Well, they—I shouldn't say that they excluded controls, but in answer to your question, I believe there are four specific circulars that are supposed to be consolidated, if you will: A-71, including Transmittal Memorandum No. 1; is it A-108? Help me out here. And two others—109 and one other.

Mr. **Podell**. And 121, on cost.

Mr. **Reed**. On cost.

The important point that I am making is that it seemed to obviously exclude A-123, which is a policy that was just issued, incidentally, this September on internal controls. And somehow security policy and internal controls, in my opinion, are inseparable.

Mr. **Glickman**. Do you—do you have any reason in your own mind why that would be excluded?

Mr. **Reed**. I really do not.

Mr. **Glickman**. Do you think it is a function of cost, that they are concerned about the cost of security systems to the Government?

Mr. **Reed**. I really cannot respond to that.

Would you like to?

Mr. **Anderson**. Yes. The announcement in the Federal Register on September 12 was telling the country, inside the Government and outside, what they were going to do, and it just didn't have that in it. However, as the comments come in, I would imagine that other people would point that out to them and that they would incorporate that A-123.

Mr. **Glickman**. Well, again I go back to the fact that—I want to make sure that we have a situation where citizens have confidence that their records and the information that the Government collects on them is used properly.

Do you see a danger that citizens will lose confidence in the Government in its efforts to collect information on citizens as a result of concern over the security of computers and the information that is contained therein?

Mr. **Reed**. I hesitate to make a generalization in responding to that sort of question. I do think that certainly the probability with time of losing the confidence of the general public certainly increases, particularly if we—if our progress, say, from here on is not more focused and constructive and more successful than it has been up until now.

And that is probably as far as I could go. I don't think we are at an alarming stage now in terms of the confidence of our citizens in Government, but I think very clearly, as time goes on, because the threats and problems, in my opinion, are going to increase, we run that risk.

Mr. **Glickman**. You mention that you think that the greatest issue is one of management.

Mr. **Reed**. Yes, sir.

Mr. **Glickman**. You are not overlooking the technology side of the picture?

Mr. **Reed**. No, sir, I sure am not. That is a very important part. I think one of your earlier witnesses, Mr. Parker, put it well. Technology is a very important part, and technologists like to advance technology solutions. And sometimes we overlook the very important part of human control that is required, the management problem. We leave the management solutions to technologists, and sometimes we pay the price for doing that.

Mr. **Glickman**. Let me just go into one system again, back to the Social Security Administration. Are you familiar with any changes that they have made in their computer security over the last several years?

Mr. **Reed**. One of the principal changes—and that is one that we reported on earlier—it happened to be in gross violation, their system, of what I would call the one category of control, physical control. Its computer facility was not conducive to good protective measures, and what they have done is established a new building to house the computers, et cetera, with much better controls.

That really is the extent of my familiarity with the system. Can you elaborate on that, Wally?

Mr. **Anderson**. I think it probably is about 1976 or so that we did a short investigation of the social security system, with the idea that they needed many new computers and a new building to house them. We concluded that the need for the new computers was not as great as the need for a new building to protect them better. Over the period of years at great expense, they now have a new building, which is a much better physical facility.

The problem of personnel, the human factors, of course, remains as a standing problem. And I think this is what Warren was talking about. The management attention has to be directed toward the human factors.

Mr. **Podell**. One other item. We have also reported on many of their technical problems, on information security. In particular, we have developed software, which we call integrated test facilities software, that we have operated within the production of environment of social security systems, and this software has helped the Administration identify errors.

The integrated test facilities software is like an online audit sampling as you are producing payment checks. We have shown cases of, in our opinion, overpayments, as well as some underpayments. And I think this has helped at least in one or two of their programs get a better handle on their error rate.

At one time they had a very large error rate. For example, in their supplementary security income program that we have reported on time and time again, in the early years they had a high error rate and were losing millions and millions of dollars because of these recontrols and because of source data errors.

Mr. **Glickman**. What about the problem of accessing into their computers, third parties accessing into their computers? To your knowledge, has that been a problem?

Mr. **Anderson**. We know of no huge problem in that respect with Social Security. Most—here their antiquated methods fall in their favor. They are mostly a large batch, tape-operated systems resident within the building.

Mr. **Glickman**. You say the old systems fall in their favor?

Mr. **Anderson**. I mean the security aspects of a self-contained, dedicated system with no terminal access to the master file is in the favor of high security.

Mr. **Podell**. We have reported on a few cases where Social Security has gone through remote telecommunications systems and remote terminals for their operators. One case we reported on, there was over $100,000 stolen from a terminal by one of the operators, and that was one of three cases prosecuted by Social Security; I might add successfully prosecuted.

In the example that I mentioned of supplemental security income program, we pointed out that the use of manual override to correct some of the high errors that I just mentioned was an excellent opportunity for employee fraud because the employees at the time could effectively erase their audit trail in performing the manual override.

Mr. GLICKMAN. Has that been changed?

Mr. PODELL. I believe it has been changed.

Mr. GLICKMAN. Do you have any estimates as to the size of Government losses because of poor computer security?

Mr. REED. We have estimates, but certainly no aggregated estimates that I think would give a sense of just how big the problem is. I would also say that probably the unreported estimates probably are significant and we, of course, have no knowledge on those, either.

Mr. GLICKMAN. When you say the unreported incidents are significant, unreport——

Mr. REED. Un—excuse me.

Mr. GLICKMAN. Go ahead.

Mr. REED. I meant undetected.

Mr. GLICKMAN. Undetected?

Mr. REED. Yes.

Mr. GLICKMAN. Do you have any reason to believe that certain agencies of Government have more undetected reported—unreported errors than other agencies?

Mr. REED. No, I don't.

Mr. GLICKMAN. Do you think it would be practical or desirable to institute a system of classifying nonnational security information in the Government?

Mr. REED. Very definitely. As a matter of fact, I believe that is the only mechanism that can be used to decide what the appropriate level of protection required for the information is. And I think it is essential.

Mr. GLICKMAN. Mr. Wright did not indicate any knowledge of this particular subject, but I am aware that there have been hearings in the past on this subject. Have you made a recommendation to anybody regarding this issue before?

Mr. REED. I will have to—I am not sure.

Mr. ANDERSON. In a sense there is an existing solution. Obviously the Privacy Act defines that kind of information that must be protected, distinguishing it from open or library information.

The Transmittal Memo No. 1 to A-71 talks about the manager level person as a security officer conducting a risk analysis. That implies that information at risk and the vulnerabilities have to be assessed and proper arrangements taken.

So I think while it may not be explicit, I think there is—there is embedded in the existing regulations things of that type.

Mr. REED. If I may, but since we apparently have no direct answer to your question, I would like to provide that one for the record.

Mr. GLICKMAN. OK.

[The information follows:]

Mr. REED. In our April 21, 1982, report, "Federal Information Systems Remain Highly Vulnerable To Fraudulent, Wasteful, Abusive, And Illegal Practices," we recommended that OMB, in part:

"Revise Circular A-71, Transmittal Memorandum No. 1, to (1) identify the minimum controls necessary for ensuring a reasonable level of protection over personal, proprietary, and other sensitive information, (2) clarify the interrelationship between Transmittal Memorandum No. 1 and policy and guidance on safeguarding information classified for purposes of national security, (3) clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary, and other sensitive information as they do to information classified for purposes of national security, and (4) establish policy and specific guidance for achieving a reasonable level of protection over those systems, using telecommunication networks."

I would like to clarify item (1) above, "identify the minimum controls necessary, et cetera." In my opinion, OMB should develop an information classification system similar to that used by the Department of Defense. OMB needs to establish classification categories, such as "nonsensitive," "sensitive," and "sensitive-critical," and then specify minimum controls to be applied in each category. For example, in the nonsensitive category, data telecommunications might not require encryption; in the sensitive category, application of the NBS Data Encryption Standard might have to be considered; and in the sensitive-critical category, National Security Agency encryption equipment and procedures could be required.

The OMB controls criteria would have to be adjusted by agencies, however, on the basis of risk analysis. For example, an agency might find that a sensitive application does not require encryption because it is transmitted by nonemanating fiber optics. On the other hand, agencies such as FBI and Treasury might find it necessary to increase the controls established for certain sensitive-critical systems.

Mr. GLICKMAN. Do you think that the roles of the Department of Defense through the NSA, and Commerce through the National Bureau of Standards, should be expanded to assist the private sector in its need for computer or communications security?

Mr. REED. First, I would say that to the degree that enhanced efforts or activity on their part can foster exchange of information, particularly on techniques, on technology, et cetera, that that should be done.

I think the converse—namely, us getting assistance from the private sector—has equal merit, and I would encourage that. There—as you know, there are some major corporations and major networks, particularly some very large international time sharing systems out there that employ fairly elaborate and, as far as we know, successful measures for information protection.

Mr. GLICKMAN. In our investigation it became clear that there may be confusion over the role of the Department of Commerce and the role of the NSA in cryptology. Can you, if you know, enlighten us as to how the roles of these agencies can be improved to aid in enhancing government use of this technology?

Mr. REED. I would like to ask Dr. Podell——

Mr. GLICKMAN. And when you talk about this, you might talk a little bit about what percentage of agencies outside of those handling classified data are presently using encryption devices and some of the related issues there.

Mr. PODELL. I think we would have to share the response to that question, but if I understand your concern about cryptology, are you talking in particular about a data encryption for communication security?

Mr. GLICKMAN. Yes.

Mr. PODELL. We have reported on the events relating to Presidential Directive 24 in one of our earlier reports. And one of the concerns we voiced was that there was no clear guidance, either for the Department of Commerce or for OMB, concerning the use of risk analysis in data telecommunications systems.

That, I understand from the previous witness, will be addressed in revising OMB Circular A-71, Transmittal Memorandum No. 1. So, that was one of our original concerns.

Also, in Presidential Directive 24, I have with me a small excerpt, unclassified excerpt, titled "National Telecommunications Protection Policy," dated February 16, 1979. It identifies a role for Commerce and a role for the National Security Agency on this same function; namely, cryptology for communications security in the United States.

It appears to me that that would have to be further investigated, and perhaps this definition of two roles for the same function and two organizations would have to be clarified and the entire Presidential directive perhaps updated.

Mr. **Glickman**. But you don't know if there has been any change since that 1979 document you referred to?

Mr. **Podell**. I have called the National Security Council and asked them when they are coming out with an update on Presidential Directive 24 and have information indications that they are considering revising this, but I have no specifics.

Mr. **Glickman**. OK. Let me ask you just a few final questions. You reported in 1980 that many Federal agencies had not adequately planned for ADP data processing disasters, and I assume that we're talking about a whole range of potential disasters, from earthquakes to, you name it, tornados, floods.

Do you believe the situation has changed, and in terms of disasters, I think we ought to also talk about power shortages, brownouts, this kind of thing.

Mr. **Reed**. I have no evidence that there's been a material change. Have you, Wally?

Mr. **Anderson**. We normally follow up our reports and we did follow up that report and we heard that the agencies plan to do a better job in backup and contingency plans.

If you recall, we went to 55 places and there wasn't a single one where we considered they were adequate in that respect. These were all unclassified civilian-type——

Mr. **Glickman**. But have you seen any evidence in the last 3 years to indicate that there's been any change in policy?

Mr. **Anderson**. Not really.

Mr. **Glickman**. And yet our use of computers is growing daily and our use and reliance on them is growing daily and probably more likely than a hacker coming in and changing my social security records, is a brown-out or a power shortage or a flood which could destroy records and yet there's been nothing done to protect those records against a natural disaster.

Mr. **Reed**. I would just like to make our response clear. I, and we, are not aware of any material progress in this area. That's not to say that maybe there has been some. We are just not aware.

Mr. **Glickman**. Well, let me ask you this question—it probably shows my ignorance in the area—do most of the agencies that keep very material records like Veterans' Administration or Social Security keep them in a duplicate form? I mean, are there duplicate computer tapes kept so as to protect the individual?

Mr. **Anderson**. Yes; that is a general practice.

Mr. **Glickman**. That is a general practice.

Mr. ANDERSON. Yes.

Mr. GLICKMAN. Is that just an informal practice that agencies——

Mr. ANDERSON. Almost all agencies have learned to do that.

Mr. GLICKMAN. OK. I'm glad they——

Mr. PODELL. I'd like to add one point.

Mr. GLICKMAN. Yes.

Mr. PODELL. In our report that we're discussing, we pointed out that is a common practice, but not sufficient because if you don't have a backup facility with a duplicate set of control software to run those tapes and discs, you don't have a continuity of operations in a disaster.

Mr. GLICKMAN. OK. You know, I'm—back in 1980, the FAA moved against an air traffic controller for allegedly removing data from computerized radar scopes and contributing to the potential endangerment of a Soviet airliner—kind of ironic—approaching Kennedy International Airport in January. That kind of problem has been reported as happening at some point in the future.

The FAA is currently embarked on the largest computer acquisition—nondefense computer acquisition in Government. Are you aware of their efforts to improve the security of those systems? Are they, in fact, moving in that area?

Mr. REED. I am not aware of the degree to which they are focusing on security as part of their modernization program, but I can tell you this, that we are initiating an audit in that area of that acquisition and we probably will be paying some attention to that area.

Mr. GLICKMAN. There is nothing that probably could be more disruptive to America than a major invasion of the air traffic control system, and so I would urge you to do that. If you need any help from our committee, we'll talk to you about it later.

One final question on legislation. Your testimony indicates your—not so much your support, but the fact that you believe that some form of computer crime legislation, vis-a-vis Federal installations, would be helpful. I wonder if you would amplify on that.

Mr. REED. Well, first—first, I—I should qualify by saying that our audit focus in this area has not been extensive, but in the one report or audit we did in this area, we did identify at least a need for one area of legislation and it had to do with the legalities of wiretapping, using electronic devices. I think I may have mentioned that in my remarks.

The Omnibus Crime Act, I think, is the one I refer to in the written statement, made—amended the Communications Act of 1934 and in doing so, clearly established aural, by ear, listening, as being illegal and excluded. At least, that's our interpretation, interception by using electronic devices.

Mr. GLICKMAN. Well, OK, I guess my—I saw that part of your statement. I was thinking more in terms of improper access into, let's say, a social security system computer is currently now probably not a Federal crime; it may not be any crime at all. I suppose if there is an intentional effort to modify data, it may be a Federal crime. If an intentional effort is to steal data, take money, it would be, but there is clearly a hybrid area where—where you may or may not have a Federal crime. If you have a sharp lawyer, he could probably get you off and it may or may not be a State crime, either.

And so, that's one of the areas we're in focus with and perhaps the establishment of Federal criminal standards in this area just might improve the operation and the management of the systems, as you mentioned in your statement.

Mr. REED. I would agree wholeheartedly.

Mr. GLICKMAN. Let me just finally talk to you—going back to—it's sometimes easy for us in Congress to go back to institutional roles but it seems to be very important in this case. It looks to me as if there is not what you call a "current assessment," agency assessment of computer security needs, problems in this Government, and that may be—I may be saying the same thing that you've said in terms of some of the policy manuals, but I wonder if you would amplify on that, particularly as to what has happened in the month of September on the establishment of new policies.

Do we have an assessment in this Government? Do we know what our computer security needs are on an agency-by-agency basis? Has it been published anywhere? Is there anybody really monitoring it?

Mr. REED. I—I think the closest—the answer is no, not to my knowledge, and the perhaps most promising activity that may move us in that direction will be the vulnerability assessments that all of the agencies are now legally responsible for coming up with. To the degree that those—to the degree that those vulnerability assessments focus on information security and their vulnerabilities, we will have a better measure of just how vulnerable we are.

Mr. GLICKMAN. And to the extent that the agencies comply with the statutes——

Mr. REED. Yes, sir.

Mr. GLICKMAN [continuing]. And if they have an Office of Management and Budget that doesn't care to prod them in complying with the statute, then we have a continuing problem.

Mr. REED. Yes, sir.

Mr. GLICKMAN. OK. Well, we sure thank you for your excellent testimony today and look forward to—continue to work with you on these issues.

Mr. REED. Our pleasure.

Mr. GLICKMAN. Our next witness is Dr. John W. Lyons, Acting Director, National Bureau of Standards, and I think you're accompanied by Dennis—Dr. Dennis Branstad, with NBS.

Dr. Lyons, it's a pleasure to have you here and you may proceed as you deem appropriate, with the knowledge that you may summarize if you wish to.

STATEMENTS OF JOHN W. LYONS, ACTING DIRECTOR, NATIONAL BUREAU OF STANDARDS; AND DENNIS BRANSTAD, MANAGER, COMPUTER INTEGRITY AND SECURITY TECHNOLOGY GROUP, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY, NATIONAL BUREAU OF STANDARDS, U.S. DEPARTMENT OF COMMERCE

Mr. LYONS. Thank you, Mr. Chairman. I am John Lyons, Acting Director of the National Bureau of Standards, and I am accompanied by Dr. Dennis Branstad on my right, your left, who is manager of the computer integrity and security technology group in the NBS Institute for Computer Sciences and Technology, ICST. We're pleased to have this opportunity to testify on the important topic of computer communication security.

I have a complete statement responding in detail to the questions in your invitation. I would like that incorporated in the record.

I would like to focus on some of your questions, giving you our perspective on the computer communication security problem, and explain what NBS has done and is doing to find solutions. The remaining questions that I will not address in my summary are addressed in the full statement.

I'd like to point out at this juncture that, as has been stated earlier by Mr. Wright, this is a coordinated program with OMB worrying about policy matters and GSA worrying about property management and other aspects of the problem. The Secretary of Commerce issues the standards and the Bureau of Standards, ICST, does technical work in this area.

ICST has played a leading role in developing standards, guidelines and publications, specifying cost-effective means for improving security in a variety of Federal and private-sector applications. I want to point that NBS is a scientific and engineering research and standards laboratory and that we have no regulatory authority.

Computer standards for Federal use are issued by the Department of Commerce as Federal information processing standards, or FIPS. We have played a lead role in working with the private, nonprofit American National Standards Institute [ANSI] to develop voluntary standards, which are frequently the basis for Federal standards.

Computer security covers a wide range of problems, ranging from accidental errors and omissions to high-technology attacks on classified systems. There is a wide range of straightforward and relatively inexpensive solutions to the computer security problems faced by businesses, Government, universities, and individuals. Between 80 and 90 percent of the problems have been addressed and could easily be avoided by using available administrative procedures and technology.

The vast majority of computer security violations have not resulted from hard technical penetrations by sophisticated criminals and could have been prevented. Every organization which uses a computer, especially those providing remote access to the computer, should be acquainted with the vulnerabilities exploited in recent incidents and every organization should consider its own vulnerabilities and related risks.

NBS has already provided assistance for use by those concerned with computer security. I have with me a listing of guidelines and standards which will help managers interested in reducing security threats. Literally thousands of people have taken advantage of regular national conferences held at NBS on computer security over the past 6 years.

I also have with me a listing of some of those activities; two lists here. I would like to submit these documents for the record, if I may.

Mr. GLICKMAN. Sure, they'll be included in the record.

[The lists of Mr. Lyons follow:]

COMPUTER SECURITY PUBLICATIONS

NBS Publications List 91

Revised June 1982

U.S. Department of Commerce
National Bureau of Standards
Institute for Computer Sciences and Technology

INSTITUTE FOR COMPUTER SCIENCES
AND TECHNOLOGY
NATIONAL BUREAU OF STANDARDS
Washington, D.C. 20234

COMPUTER SECURITY PUBLICATIONS

The security of computer systems and data is a critical concern for the Federal government which depends on computers to carry out vital functions affecting the health, safety, and security of citizens. The Institute for Computer Sciences and Technology (ICST) at the National Bureau of Standards (NBS) addresses the problems of protecting Federal computer systems and data as part of a governmentwide program directed toward improving the management and use of Federal computer resources.

Under P. L. 89-306 (Brooks Act), ICST develops Federal automatic data processing (ADP) standards and guidelines, provides scientific and technical services to other Federal agencies in the selection and use of computer technology, and conducts computer science research. In carrying these responsibilities, ICST issues Federal Information Processing Standards Publications (FIPS PUBS), guides, and other reports covering all aspects of ADP management and use. This publication list includes ICST publications dealing with computer security and risk management issues.

Information about ICST programs is available from:

Program Development Office
Institute for Computer Sciences
and Technology
Administration Building A-209
National Bureau of Standards
Washington, DC 20234
Phone: (301) 921-2834

HOW TO ORDER PUBLICATIONS

These publications are available through the Government Printing Office (GPO) and the National Technical Information Service (NTIS). The source and price for each publication are indicated. Orders for publications should include title of publication, NBS publication number (Spec. Pub. 000, Tech. Note 000, etc.) and NTIS or GPO number. You may order at the price listed; however, prices are out subject to change without notice.

Submit payment in the form of postal money order, express money order or check made out to the Superintendent of Documents for GPO-stocked documents or to the National Technical Information Service for NTIS-stocked documents.

Mailing addresses are:

Superintendent of Documents
U. S. Government Printing Office
Washington, DC 20402

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

Telephone numbers for information are:

GPO Order Desk	(202) 783-3238
NTIS Orders	(703) 487-4780
NTIS Information	(703) 487-4600

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS)

Federal Information Processing Standards Publications (FIPS PUBS) are developed by the Institute for Computer Sciences and Technology (ICST) and issued under the provisions of the Federal Property and Adminstrative Services Act of 1949, as amended; Public Law 89-306 (79 Stat. 1127); Executive Order 11717 (38 FR 12315); and Part 6 of Title 15 of the Code of Federal Regulations (CFR).

FIPS PUBS are sold by the National Technical Information Service (NTIS), U.S. Department of Commerce. A list of current FIPS covering all ICST program areas is available from:

Standards Processing Coordinator (ADP)
Institute for Computer Sciences
and Technology
Technology Building, B-64
National Bureau of Standards
Washington, DC 20234
Phone: (301) 921-3157

GUIDELINES FOR ADP PHYSICAL SECURITY AND RISK MANAGEMENT,

FIPS-PUB-31 June 1974

Order from NTIS $7.50

Provides guidance to Federal organizations in developing physical security and risk managment programs for their ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans, security awareness, and security audit. Can be used as a checklist for planning and evaluating security of computer systems.

GLOSSARY FOR COMPUTER SYSTEMS SECURITY

FIPS-PUB-39 February 1974

Order from NTIS $6.00

A reference document containing approximately 170 terms and definitions pertaining to privacy and computer security.

COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

FIPS-PUB-41 May 1975

Order from NTIS $6.00

Provides guidance in the selection of technical and related procedural methods for protecting personal data in automated information systems. Discusses categories of risks and the related safeguards for physical security, information management practices, and system controls to improve system security.

DATA ENCRYPTION STANDARD

FIPS-PUB-46 January 1977

Order from NTIS $6.00

Specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of sensitive, but unclassified, computer data. The algorithm uniquely defines the mathematical steps required to transform computer data into a cryptographic cipher and the steps required to transform the cipher back to its original form.

GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION

FIPS-PUB-48 April 1977

Order from NTIS $6.00

Discusses the performance of personal identification devices, how to evaluate them, and considerations for their use within the context of computer system security.

GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS

FIPS-PUB-65 August 1979

Order from NTIS $7.50

Presents a technique for conducting a risk analysis of an ADP facility and related assets. Provides guidance on collecting, quantifying, and analyzing data related to the frequency of caused by adverse events. This guideline describes the characteristics and attributes of a computer system that must be known for a risk analysis and gives an example of the risk analysis process.

GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS

FIPS-PUB-73 June 1980

Order from NTIS $9.00

Describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing and operating computer systems which require protection Fundamental security controls such a data validation, user identity verification, authorization, journalling, variance detection, and encryption are discussed.

GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD

FIPS-PUB-74 April 1981

Order from NTIS $7.50

Provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. For use in conjunction with FIPS PUB 46 and FIPS PUB 81.

DES MODES OF OPERATION

FIPS-PUB-81 December 1980

Order from NTIS $7.50

Defines four modes of operation for the Data Encryption Standard which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically occurrence and the damage protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL

FIPS-PUB-83 September 1980

Order from NTIS $7.50

Provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks. Describes use of passwords, identification tokens, verification by means of personal attributes, identification of remote devices, role of encryption in network access control, and computerized authorization techniques.

GUIDELINES FOR ADP CONTINGENCY PLANNING

FIPS-PUB-87 March 1981

Order from NTIS $7.50

Describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN DATABASE APPLICATIONS

FIPS PUB 88 August 1981

Order from NTIS $10.50

Provides explicit advice on achieving database integrity and security control. Identifies integrity and security problems and discusses procedures and methods which have proven effective in addressing these problems. Provides an explicit, step-by-step procedure for examining and verifying the accuracy and completeness of a database.

SPECIAL PUBLICATIONS AND OTHER REPORTS

These publications present the results of ICST studies, investigations, and research on computer security and risk management issues. Publications are sold by either the Government Printing Office or the National Technical Information Service as noted for each entry.

SPECIAL PUBLICATIONS

Accessing Individual Records from Personal Data Files Using Nonunique Identifiers

By Gwendolyn B. Moore, John L. Kuhns, Jeffrey L. Treffzs and Christine A. Montgomery

NBS Spec. Pub 500-2 February 1977
Order from NTIS as PB263176 $18.00

Analyzes methodologies for retrieving personal information using nonunique identifiers such as name, address, etc. This study presents statistical data for judging the accuracy and efficiency of various methods.

The Use of Passwords for Controlled Access to Computer Resources

By Helen Wood
NBS Spec. Pub. 500-9 May 1977

Order from GPO as SN 003-003-01770-1
$2.00

Describes the need for and uses of passwords. Password schemes are categorized according to selection technique, lifetime, physical characteristics and information content. Password protection and cost considerations are discussed. A glossary and annotated bibliography are included.

A Data Base Management Approach to Privacy Act Compliance

By Elizabeth Fong
NBS Spec. Pub. 500-10 June 1977

Order from GPO as SN 003-003-01787-6
$1.40

Discusses how commercially available data base management systems can be used to implement Privacy Act requirements for the handling of personal data.

GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION

FIPS-PUB-48 April 1977

Order from NTIS $6.00

Discusses the performance of personal identification devices, how to evaluate them, and considerations for their use within the context of computer system security.

GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS

FIPS-PUB-65 August 1979

Order from NTIS $7.50

Presents a technique for conducting a risk analysis of an ADP facility and related assets. Provides guidance on collecting, quantifying, and analyzing data related to the frequency of caused by adverse events. This guideline describes the characteristics and attributes of a computer system that must be known for a risk analysis and gives an example of the risk analysis process.

GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS

FIPS-PUB-73 June 1980

Order from NTIS $9.00

Describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing and operating computer systems which require protection Fundamental security controls such a data validation, user identity verification, authorization, journalling, variance detection, and encryption are discussed.

GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD

FIPS-PUB-74 April 1981

Order from NTIS $7.50

Provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. For use in conjunction with FIPS PUB 46 and FIPS PUB 81.

DES MODES OF OPERATION

FIPS-PUB-81 December 1980

Order from NTIS $7.50

Defines four modes of operation for the Data Encryption Standard which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically occurrence and the damage protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL

FIPS-PUB-83 September 1980

Order from NTIS $7.50

Provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks. Describes use of passwords, identification tokens, verification by means of personal attributes, identification of remote devices, role of encryption in network access control, and computerized authorization techniques.

GUIDELINES FOR ADP CONTINGENCY PLANNING

FIPS-PUB-87 March 1981

Order from NTIS $7.50

Describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN DATABASE APPLICATIONS

FIPS PUB 88 August 1981

Order from NTIS $10.50

Provides explicit advice on achieving database integrity and security control. Identifies integrity and security problems and discusses procedures and methods which have proven effective in addressing these problems. Provides an explicit, step-by-step procedure for examining and verifying the accuracy and completeness of a database.

SPECIAL PUBLICATIONS AND OTHER REPORTS

These publications present the results of ICST studies, investigations, and research on computer security and risk management issues. Publications are sold by either the Government Printing Office or the National Technical Information Service as noted for each entry.

SPECIAL PUBLICATIONS

Accessing Individual Records from Personal Data Files Using Nonunique Identifiers

By Gwendolyn B. Moore, John L. Kuhns, Jeffrey L. Treffzs and Christine A. Montgomery

NBS Spec. Pub 500-2 February 1977
Order from NTIS as PB263176 $18.00

Analyzes methodologies for retrieving personal information using nonunique identifiers such as name, address, etc. This study presents statistical data for judging the accuracy and efficiency of various methods.

The Use of Passwords for Controlled Access to Computer Resources

By Helen Wood
NBS Spec. Pub. 500-9 May 1977

Order from GPO as SN 003-003-01770-1
$2.00

Describes the need for and uses of passwords. Password schemes are categorized according to selection technique, lifetime, physical characteristics and information content. Password protection and cost considerations are discussed. A glossary and annotated bibliography are included.

A Data Base Management Approach to Privacy Act Compliance

By Elizabeth Fong
NBS Spec. Pub. 500-10 June 1977

Order from GPO as SN 003-003-01787-6
$1.40

Discusses how commercially available data base management systems can be used to implement Privacy Act requirements for the handling of personal data.

Audit and Evaluation of Computer Security
Edited by Zella Ruthberg and Robert McKenzie
NBS Spec. Pub. 500-19 October 1977

Order from GPO as SN 003-003-01848-1
$4.00

Reports on the recommendations of audit and computer experts to improve computer security audit procedures. Subjects covered include audit standards, administrative and physical controls, program and data integrity, and audit tools and techniques.

Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard
By Jason Gait
NBS Spec. Pub. 500-20 November 1977

Order from GPO as SN 003-003-00249-7
$2.25

Desribes the design and operation of the NBS testbed that is used for the validation of hardware implementations of the Data Encryption Standard (DES). This report provides the full specification of the DES algorithm, a complete listing of the DES test set and a detailed description of the interface to the testbed.

Design Alternatives for Computer Network Security (vol. 1)
The Network Security Center: A System Level Approach to Computer Network Security (vol. 2)
By Gerald D. Cole and Frank Heinrich
NBS Spec. Pub. 500-21 January 1978

Order from GPO as SN 003-003-01881-3
$6.00

This two-volume study covers network security requirements and design and implementation requirements of a special computer dedicated to network security. The approach utilizes a dedicated minicomputer to check authentication of network users, and, to some extent, to check authorization. The study focuses on use of the Data Encryption Standard to protect network data and recommends procedures for generating, distributing and protecting encryption keys.

Performance Assurance and Data Integrity Practices
By Robert L. Patrick
Edited by Robert P. Blanc
NBS Spec. Pub. 500-24 January 1978

Order from GPO as SN 003-003-01879-1
$2.20

Details practices and methods that have been successful in preventing or reducing computer system failures caused by programming and data errors. The methods described cover large data processing applications, scientific computing applications, programming techniques and systems design.

An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse
By Brian Ruder and J. D. Madden
Edited by Robert P. Blanc
NBS Spec. Pub. 500-25 January 1978

Order from GPO as SN 003-003-01871-6
$2.40

Analyzes 88 computer safeguard techniques that could be applied to recorded actual computer misuse cases. Presents a model for use in classifying and evaluating safeguards as mechanisms for detecting and preventing misuse.

Computer Security and the Data Encryption Standard
Edited by Dennis Branstad
NBS Spec. Pub. 500-27 February 1978

Order from GPO as SN 003-003-01891-1
$3.00

Includes papers and summaries of presentations made at a 1977 conference on computer security. Subject areas are physical security, risk assessment, software security, computer network security, applications and implementation of the Data Encryption Standard.

Considerations in the Selection of Security Measures of Automatic Data Processing Systems
By Michel J. Orceyre and Robert H. Cortney, Jr.
Edited by Gloria R. Bolotsky
NBS Spec. Pub. 500-33 June 1978

Order from GPO as SN 003-003-01946-1
$1.40

Details methods and techniques for protecting data processed by computer and transmitted via telecommunications lines. This report identifies the controls that can be instituted to protect ADP systems when risks and potential losses have been identified.

Computers, Personnel Administration, and Citizen Rights
By Alan F. Westin
NBS Spec. Pub. 500-50 July 1979

Order from GPO as SN 003-003-02087-7
$8.00

Reports on the impact of computers on citizen rights in the field of personnel recordkeeping. This study traces the changing patterns of employment and personnel administration and examines the trends in computer use in personnel administration. It recommends policy actions to guide the management of personnel systems that respect citizen rights.

A Key Notorization System for Computer Networks
By Miles E. Smid
NBS Spec. Pub. 500-54 October 1979

Order from GPO as SN 003-003-02130-0
$1.75

Describes a system for key notorization, which can be used with an encryption device, to improve data security in computer networks. The key notorization system can be used to communicate securely between two users, communicate via encrypted mail, protect personal files, and provide a digital signature capability.

Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls
Edited by Zella G. Ruthberg
NBS Spec. Pub. 500-57 April 1980

Order from GPO as SN 003-003-02178-4
$6.00

Proceedings of the second NBS/GAO workshop to develop improved computer security audit procedures. Covers eight sessions: three sessions on managerial and organizational vulnerabilities and controls and five technical sessions on terminals and remote peripherals, communication components, operating systems, applications and non-integrated data files, and data base management systems.

Maintenance Testing for the Data Encryption Standard
By Jason Gait
NBS Spec. Pub. 600-61 August 1980

Order from GPO as SN 003-003-02225-0
$2.00

Describes four tests that can be used by manufacturers and users to check the operation of data encryption devices. These tests are simple, efficient, and independent of the implementation of the Data Encryption Standard (FIPS 46).

The SRI Hierarchical Development Methodology (HDM) and its Application to the Development of Secure Software
By Karl N. Levitt, Peter Neumann, and Lawrence Robinson
NBS Spec. Pub. 500-67 October 1980

Order from GPO as SN 003-003-02258
$3.75

Describes the SRI Hierarchical Development Methodology for designing large software systems such as operating systems and data management systems that must meet stringent security requirements.

Executive Guide to ADP Contingency Planning
By James K. Shaw and Stuart W. Katzke
NBS Spec. Pub. 500-85 July 1981

Order from NTIS as PB 82 165226
$6.00

This document provides, in the form of questions and answers, the background, and basic essential information required to understand the developmental process for automatic data processing (ADP) contingency plans. The primary intended audience consists of executives and managers who depend on ADP resources and services, yet may not be directly responsible for the daily management or supervision of data processing activities or facilities.

OTHER REPORTS

A Computer Model to Determine Low Cost Techniques to Comply With the Privacy Act of 1974
By Robert C. Goldstein and Henry H. Seward
NBSIR 76-985 February 1976

Order from NTIS as PB 250755 $4.50

Presents a computer model to simulate costs of implementing the Privacy Act and to identify differences in cost that result from alternative approaches to implementing mandated safeguards. The computer model can be modified to reflect changing circumstances and different recordkeeping systems.

Security Analysis and Enhancements of Computer Operating Systems
Edited by Theordore Linden
NBSIR 76-1041 April 1976

Order from NTIS as PB 257087 $9.00

Examines types of security problems that arise in operating systems and suggests ways to improve security. Three commercial systems are analyzed, and security flaws are classified.

A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements
NBS Tech. Note 906 June 1976

Order from GPO as SN 003-003-01630-6
$1.35

Identifies the actions required of recordkeepers to comply with the Privacy Act and estimates the cost of these actions. Includes a computer model to aid in the selection of cost-effective safeguards.

Operating System Structures to Support Security and Reliable Software
By Theodore Linden
NBS Tech. Note 919   August 1976

Order from GPO as SN 003-003-01658-6
$1.25

Examines techniques to improve the design of computer systems. This study focuses on two system structuring concepts using modular software structures to satisfy security requirements and make systems more reliable.

Data Base Directions: The Next Steps
Edited by John Berg
NBS Spec. Pub. 451   September 1976

Order from GPO as SN 003-003-01662-4
$3.00

Proceedings of a workshop held in 1975 to develop information about data base technology for managers of data base systems. Covers five subject areas: auditing, evolving technology, government regulations, standards and user experiences.

Report on the Workshop on Estimation of Signifcant Advances in Computer Technology
Edited by Paul Meissner
NBSIR 76-1189   December 1976

Order from NTIS as PB 279373 $7.50

Reports on a 1976 workshop held to solicit information on computer technology advances with potential impact on the security of the Data Encryption Standard. Presents the evaluations of computer industry, academic and government experts on computer system design, architecture and manufacturing.

Computers, Health Records, and Citizen Rights
By Alan F. Westin
NBS Monograph 157   December 1976

Order from GPO as SN 003-003-01681-1
$4.55

Reports on the impact of computers on citizen rights in the health recordkeeping area. This study looks at the uses made of personal medical data and the trends in computerization of data. It recommends policy actions to guide the management of health data systems that respect citizen rights.

A Policy Analysis of Citizen Rights Issues in Health Data Systems
By Alan F. Westin and Florence Isbell
NBS Spec. Pub. 469   January 1977

Order from GPO as SN 003-003-01730-2
$1.05

A condensation of "Computers, Health Records, and Citizen Rights" (Monograph 157).

Report of the Workshop on Cryptography in Support of Computer Security
By Dennis Branstad, Jason Gait and Stuart Katzke
NBSIR 77-1291   September 1977

Order from NTIS as PB 271744 $9.00

Reports on a workshop held at NBS to obtain expert opinions on the mathematical and statistical characteristics of the Data Encryption Standard. Summarizes the formal presentations and outlines the major issues that were raised.

SUBJECT INDEX

	Page
Contingency Planning	
FIPS PUB 87	4
SPEC PUB 500-85	7
Database Security	
FIPS PUB 88	4
SPEC PUB 451	8
Encryption	
FIPS PUB 46	2
FIPS PUB 74	3
FIPS PUB 81	3
SPEC PUB 500-20	5
SPEC PUB 500-27	6
SPEC PUB 500-54	6
SPEC PUB 500-61	6
NBSIR 76-1189	8
NBSIR 77-1291	8
Evaluation of Computer Security	
SPEC PUB 500-19	5
SPEC PUB 500-57	6
General Computer Security	
FIPS PUB 39	2
FIPS PUB 73	3
SPEC PUB 500-24	5
SPEC PUB 500-25	5
SPEC PUB 500-33	6
NBSIR 76-1189	8
Network Security	
SPEC PUB 500-21	5
SPEC PUB 500-33	6
SPEC PUB 500-54	6

	Page
Physical Security	
FIPS PUB 31	2
Privacy	
FIPS PUB 41	2
SPEC PUB 500-10	4
SPEC PUB 500-50	6
NBSIR 76-985	7
TECH NOTE 906	7
Monograph 157	8
SPEC PUB 469	8
Risk Management	
FIPS PUB 31	2
FIPS PUB 65	3
Software and Operating Systems	
SPEC PUB 500-2	4
SPEC PUB 500-24	5
SPEC PUB 500-25	5
SPEC PUB 500-67	7
NBSIR 76-1041	7
TECH NOTE 919	8
User Authentication	
FIPS PUB 48	3
FIPS PUB 83	3
SPEC PUB 500-9	4

INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY

SELECTED

COMPUTER SECURITY AND RISK MANAGEMENT ACTIVITIES

1980 - PRESENT

ICST SPONSORED CONFERENCES, SEMINARS, AND WORKSHOPS:

Annual Seminar on the Security of Federal ADP Systems, co-sponsored with the Federal ADP Users Group (June 1980, 1981, 1982, and 1983).

First Seminar on the Department of Defense Computer Security Initiative, co-sponsored with the Department of Defense, July 17-18, 1979, National Bureau of Standards, Gaithersburg, MD.

Second Seminar on the Department of Defense Computer Security Initiative, co-sponsored with the Department of Defense, January 15-17, 1980, National Bureau of Standards, Gaithersburg, MD.

Third Seminar on the Department of Defense Computer Security Initiative, co-sponsored with the Department of Defense, November 1980, National Bureau of Standards, Gaithersburg, MD.

Fourth Seminar on the Department of Defense Computer Security Initiative, co-sponsored with the Department of Defense, August 10-12, 1981, National Bureau of Standards, Gaithersburg, MD.

Fifth Seminar on the Department of Defense Computer Security Initiative, co-sponsored with the Department of Defense, May 24-26, 1982, National Bureau of Standards, Gaithersburg, MD.

Sixth Department of Defense - National Bureau of Standards Conference on Computer Security, to be held November 15-17, 1983, National Bureau of Standards, Gaithersburg, MD.

Workshop on Users Access Authorization, February 26-27, 1981, National Bureau of Standards, Gaithersburg, MD.

Workshop on Risk Analysis, May 29, 1980, National Bureau of Standards, Gaithersburg, MD.

Seminar on Computer Security Certification for Federal Agencies, July 12, 1982, National Bureau of Standards, Gaithersburg, MD.

Workshop on Certification of Computer Security, December 14, 1981, National Bureau of Standards, Gaithersburg, MD.

Workshop on Certification of Computer Security, April 2, 1981, National Bureau of Standards, Gaithersburg, MD.

Workshop on Computer Security Audit for the General Auditor, January 23, 1981, National Bureau of Standards, Gaithersburg, MD.

EXTERNAL PUBLICATIONS:

"Security of Personal Computers and Office Automation," Dennis D. Steinauer, Data Security Management Series, Auerback Press, November 1983.

Cryptographic Key Notarization Methods and Apparatus, Patent, co-invented by Miles E. Smid and Dennis K. Branstad, 1983.

"Integrating the Data Encryption Standard into Computer Networks," Miles E. Smid, IEEE Transactions on Communications, Vol. Com-29, No. 6, June 1981.

"Authentication Using the Federal Data Encryption Standard, Miles E. Smid, Proceedings of the National Electronics Conference, October 1981.

American National Standard for Financial Institution Message Authentication, Miles E. Smid, co-authored as a member of ANSI X9E8 Working Group, ANSI X9.9 - 1982, April 13, 1982.

Integrity and Security Standards Based on Cryptography, Dennis K. Branstad and Miles E. Smid, Computers & Security, Vol. 1, No. 3, November, 1982.

"American National Standard for Financial Institution Key Management," Miles E. Smid, co-authored as a member of X9E9 ANSI Working Group, to be published.

"Public Cryptography Outlook," Miles E. Smid, Proceedings of the ACM, New York, October 24-26, 1983.

"Certification and Accreditation: Quality Control for DP Security," Zella G. Ruthberg and William Neugent, Data Security Management Series, Auerbach Publishing Co., March 1983.

"A Question of Leadership," Zella G. Ruthberg, Datamation, February 1983.

A quarterly column on computer security management and technical controls, Zella G. Ruthberg, The EDP Auditor, Journal of the EDP Auditors Foundation.

"Risk Assessment and Managerial Analysis," The EDP Auditor, Journal of the EDP Auditors' Foundation, Fall 1980.

"An Executive Guide to ADP Contingency Planning," James Shaw and Stuart W. Katzke, Computers and Security, Vol. 1, No. 3, November 1982.

"Federal Standards in Risk Analysis and Contingency Planning," Susan K. Reed and Stuart W. Katzke, Data Management, Vol. 18, No. 1, January 1980.

"Communications Security for Electronic Funds Transfer Systems," *IEEE Transactions on Communications*, Jason Gait and Dennis K. Branstad, (in progress).

"Computer Security Integrity Technology," Dennis K. Branstad, *Proceedings of the Fifth Seminar on the DoD Computer Security Initiative*, May 1982.

"The Computer Security and Risk Management Program," Stuart W. Katzke, *Proceedings of the Fifth Seminar on the DoD Computer Security Initiative*, May 1982.

"Computer Security Evaluation and Certification," Zella G. Ruthberg, *Proceedings of the Fifth Seminar on the DoD Computer Security Initiative*, May 1982.

"Reflections on Ten Years of Computer Security," Susan K. Reed and Dennis K. Branstad, *Computers and Security*, Vol. 1, No. 3, November 1983, North Holland Publishing Co.

Modes of Operation of the Data Encryption Algorithm, Dennis K. Branstad, Technical Editor, ANSI X3.106-1983, American National Standards Institute, May 16, 1983.

The Data Encryption Algorithum, Dennis K. Branstad, Technical Editor, ANSI X3.92-1981, American National Standards Institute, January 1981.

Personal Identification Number (PIN) Management and Security, Dennis K. Branstad, ANSI X9.8-1982, Member of ANSI X9A3, 1982.

Link Encryption Standard, Dennis K. Branstad, ANSI X3.105-1983, Member of ANSI X3T1, 1983.

PRESENTATIONS:

"Introduction to Small Computers for the EDP Auditor," Dennis D. Steinauer, EDP Auditors Association, Washington, DC, January 25, 1983.

"Conducting Security Reviews," Dennis D. Steinauer, State Department Embassy Security Officers Course, Washington, DC, February 22, 1983.

"Small Systems Security," Dennis D. Steinauer, Panel Presentation, Federal DP Expo, Washington, DC, April, 13, 1983.

"Security Considerations for Small ADP Systems," Dennis D. Steinauer, Federal ADP Users Group, Washington, DC, April 26, 1983.

"Technical Controls for Personal Computers," Dennis D. Steinauer, Federal ADP Users Group Annual Security Conference, Gaithersburg, MD, June 22, 1983.

"NBS Security Program and Small Systems Security Project," Dennis D Steinauer, NALTOACS Conference, China Lake, CA, July 12, 1983.

"Security of Small Computer Systems," Dennis D. Steinauer, DoD Computer Institute, Washington, DC, August 19, 1983.

"ADP Security at USDA," Dennis D. Steinauer, Videotaped Discussion for USDA training, August 30, 1983.

"Technical Security Issues for Small Systems," Dennis D. Steinauer, IEEE COMPCON Fall 83, Washington, DC, September 29, 1983.

"DES-81," Miles E. Smid, Crypto 81 Workshop, University of Southern California, CA, August 1981.

"Applications of DES," Dennis K. Branstad and Miles E. Smid, Sandia Laboratories, October 1980.

"Considerations in the Selection of a DES Cryptoperiod," Miles E. Smid, October 1980.

"Guideline for Computer Security Certification and Accreditation," Zella G. Ruthberg, presented at:

- Fourth EDP Security Officers Seminar for the Department of Agriculture, Rosslyn, VA, September 21, 1982.
- Washington Chapter of the Institute of Internal Auditors, January, 19, 1983.
- New York Chapter of the EDP Auditors Association, April 11, 1983.
- Institute of Internal Auditors 42nd International Conference, June 15, 1983, Jerusalem, Israel.
- Workshop for Computer Security Institute Annual Conference, November 7, 1983.

"Information Security: Future Issues for Office Automation and the New Cottage Industry," Zella G. Ruthberg, Workshop at the 4th Computer Security Conference of the Computer Security Institute, New York City, November 10, 1982.

"Can Sensitive Applications Be Certified?," Zella G. Ruthberg, Seminar on Security of Federal Automated Information Systems, sponsored by Federal ADP Users Group, SIG on Audit and Security, June 4, 1982, Washington, DC.

"FIPS Guidelines for Computer Security Evaluation and Certification," Zella G. Ruthberg, Seminar on Security of Federal Automated Information Systems, sponsored by Federal ADP Users Group, SIG on Audit and Security, June 3, 1981, Washington, DC.

"Risk Assessment and Managerial Analysis," Zella G. Ruthberg, EDP Auditors Association 8th International Conference, June 16-17, 1980, Mexico City, Mexico.

"Computer Security and Risk Management," Stuart W. Katzke, presented at:

- Pittsburgh Large Users Group Subgroup on Security, April 1983.
- Ohio-Kentucky-Indiana Security Group, February 1983.
- Delaware Valley Disaster Recovery Information Exchange Group, January 1983.

"Computer Security Framework," Stuart W. Katzke, January 1983, National Bureau of Standards, Gaithersburg, MD.

"Federal Computer Security Program," Stuart W. Katzke, presented at:

- Bay Area Computer Security Interest Group, San Francisco, CA, August 1982.
- Information System Security Association, Los Angeles, CA, August 1982.

"Maintaining Control of Computer Applications Via Management," Stuart W. Katzke, Third Annual Seminar on Security of Federal Automated Information Systems, FADPUG SIG on Security and Audit, June 1982.

"Security Evaluation and Management Guidelines," Stuart W. Katzke, Second Annual Seminar on Security of Federal Automated Information Systems, FADPUG SIG on Security and Audit, June 1981.

"Computer Security," Stuart W. Katzke and Dennis Branstad, Honeywell Privacy and Security Symposium, April 1982.

"Security for Computer Applications," Stuart W. Katzke, Conference on Security of Federal Automated Information Systems, FADPUG SIG on Security and Audit, June 1980.

"Legal and Technical Means of Preventing Computer Crime," Stuart W. Katzke, A Symposium and Debate, MIT Club of Washington and the Computer Law Association, November 1982.

"Data Security: A-71 Progress Report," Stuart W. Katzke, Federal DP Expo, April 1981.

"Federal Government Computer Applications: Can They Be Made Secure," Stuart W. Katzke, DHHS Systems Security Officer Meeting, November 1981.

"Security Considerations in Computer Applications," Stuart W. Katzke, Air Force Computer Security Workshop, March 1982, Gunter AFS, Montgomery, Alabama.

"Institute for Computer Sciences and Technology's Computer Security and Data Management Programs," Stuart W. Katzke, UCLA National Conference on Data Base Information Systems, Los Angeles, CA, August 23, 1982.

"Integrity and Security in Computer Networks," Dennis K. Branstad, Computer Security Institute Annual Conference, November 1982.

"Cryptography and Computer Security," Dennis K. Branstad, Network 80, January 30, 1980.

"Data Cryptography," Dennis K. Branstad, George Washington University, February 25, 1980.

Computer Network Security," Dennis K. Branstad, Federal DP Expo, April 28, 1980.

"History of the Data Encryption Standard," Dennis K. Branstad, SRI Workshop on Cryptography, July 11, 1980.

"NBS Computer Network Security Project," Dennis K. Branstad, DoD Computer Institute, October 1980; January 14, 1981; June 26, 1981.

"Electronic Funds Transfer Security," Dennis K. Branstad, EDP Auditors Association, October 14, 1980.

"Security in Computer Networks," Dennis K. Branstad, Computer Networking Conference, December 10, 1980.

"Communications Security with the DES," Dennis K. Branstad, Federal Emergency Management Agency, March 5, 1981.

"X3T1 Encryption Progress Report," Dennis K. Branstad, Computer and Business Equipment Manufacturers Association, March 1981.

"Introduction to Computer Security," Dennis K. Branstad, National Bureau of Standards, Special Lecture, July 1981.

"Computer Network Security Session," Dennis K. Branstad, Lake Arrowhead Conference, September 11, 1981.

"DES Update," Dennis K. Branstad, Honeywell Security Conference, November 2, 1981.

"Computer Cryptography," Dennis K. Branstad, George Washington University Colloquim, December 3, 1981; April 7, 1983; September 22, 1983.

"DES Security in Commercial Networks," Dennis K. Branstad, Defense Communications Agency, December 1981.

"NBS Network Security Project," Dennis K. Branstad, International Association for Computer Systems Security, June 8, 1982.

"Public Cryptography," John P. Riganati, NSA Advisory Board, September 16, 1982.

"DES Overview," Dennis K. Branstad, Government Microcircuit and Component Conference, November 4, 1982.

"Computers and Network Security," Dennis K. Branstad, George Mason University, November 1982.

"DES in Non-DoD Networks," Dennis K. Branstad, Defense Communications Agency, December 1, 1982.

"Integrity and Security in Financial Networks," Dennis K. Branstad, American Bankers Association Telecommunications Conference, February 8, 1983.

"New Directions in Security," Dennis K. Branstad, Data Communications Conference, April 28, 1983.

"Security Considerations in Optical Digital Data Disks," Dennis K. Branstad, NBS Workshop, June 1983.

"Security of Financial Networks," Dennis K. Branstad and Miles E. Smid, Niagra Falls Savings Bank, July 12, 1983.

"Safeguard Standards in EFT Networks," Dennis K. Branstad, DCI Security Meeting, July 15, 1983.

OTHER PROFESSIONAL ACTIVITIES:

EDP Auditors Association, National Capital Area Chapter, Dennis D. Steinauer, Chapter Secretary and 1983 Professional Development Seminar Coordinator

ACM, Special Interest Group on Security Audit and Control, Standards Review Subgroup, Stuart W. Katzke and Dennis K. Branstad, Group Leaders, and Zella G. Ruthberg, Member.

EDP Auditors Association, Interprofessional Liaison Committee, Zella G. Ruthberg and Stuart W. Katzke, Members.

Computer Security Alert Newsletter, Zella G. Ruthberg, Advisory Board.

Seminar on Security of Federal Automated Information Systems, Stuart W. Katzke, Session Chairperson, June 1983, National Bureau of Standards, Gaithersburg, MD.

COMPCON Fall 83, Stuart W. Katzke, Session Chairperson, September 1983, Crystal City, VA.

"President's Council on Integrity and Efficiency Computer Audit Study Group," Invited Workshop, Stuart W. Katzke and Zella G. Ruthberg, December 1982, Quantico, VA.

"Computer Security for the Commercial World," IEEE Workshop, Stuart W. Katzke and Dennis K. Branstad, July 1981, Lake Arrowhead, CA.

Computers and Security, North Holland Publishing Co., Stuart W. Katzke, Editorial Board.

ANSI X3T1, Technical Committee on Data Encryption, Dennis K. Branstad, Chairman/Member, 1978-Present.

ANSI X9A3, Subcommittee on Bankcard Security, Dennis K. Branstad, Vice-Chairman/Member, 1979-1981.

ANSI X9E8, Subcommittee on Financial Institution Message Authentication, Miles E. Smid, Member, 1979-1982.

ANSI X9E9, Subcommittee on Financial Institution Cryptographic Key Management, Miles E. Smid and Elaine Barker, Members, 1982-Present.

DCI Safeguards Study Group, Dennis K. Branstad and Elaine Barker, Members, 1983.

American Bankers Association Bankcard Security Committee, Dennis K. Branstad, Government Liaison, 1980-Present.

Mr. LYONS. A considerable amount of basic work to develop computer security solutions has been done already and we are continuing. Our next workshop on the subject is scheduled for mid-November of this year.

We have published or are about to publish documents containing technical information and administrative guidance for computer security in a number of areas. These include risk assessment, a procedure for estimating potential losses related to accidents or intentional misuse of ADP systems.

Based on a formal risk assessment, computer safeguards can be selected which provide an appropriate balance among security, cost-effectiveness, and residual risk.

NBS has also been concerned with, and is providing information on self-certification and accreditation of safeguards, contingency planning to assure continuity of ADP services should an unexpected event occur, and security for small systems.

The widespread use of personal and professional computers and computer-based word processors has raised questions about the security requirements and capabilities of small systems. We are now investigating these issues.

The fundamental requirement for controlling access to computer systems and networks is being able to identify authorized uses. Over the past several years, we have investigated fingerprint readers, voice recognizers, automated human signature verifiers, hand geometry readers, and palm print readers. These devices rely on accurately differentiating among people, based on a particular physical chartacteristic.

Passwords are the least expensive method of identifying computer users and if properly implemented and used, provide a reasonable level of initial access control for a distributive computer system or network. We are completing a proposed standard on password usage which specifies 10 factors and related security criteria that must be considered when designing and implementing a password system.

In terms of computer communications security, our goal is widespread availability of cost-effective technology. Telecommunications security standards are necessary to assure that requested access to a computer in any network is authorized, that the data being translated are not disclosed or modified without authorization, and that the terminal and the computer are mutually authenticated.

ICST initiated a program in 1973 to establish a series of standards for assuring the integrity and security of computer networks. This cooperative program between Government and industry has resulted in Federal and ANSI standards. One of the most important in this series is the Data Encryption Standard, or DES, published in 1977.

This standard specifies a cryptographic algorithm for the protection of unclassified, but sensitive computer data. The algorithm was developed in the private sector, submitted to NBS in response to a public solicitation for such algorithms and reviewed by the National Security Agency at our request.

This standard has been widely adopted, was published by ANSI, and is recommended for use by the American Bankers' Association for protecting electronic funds tranfers. We have with us several DES chips, or electronic devices for encrypting and decrypting texts. Complete DES systems are now available commercially for as little as $250.

Working closely with ANSI, we have published, or soon will publish, other standards that directly address telecommunications security needs. These include our DES modes of operation standard, an upcoming data integrity standard, an upcoming network security publications on how to control a user's access once he has entered the computer system.

As computer networks and distributive processing become even more commonplace, it will be more important that computer managers use these standards and management tools to prevent exploitation of the generic vulnerabilities of computer networks.

While much of the technology needed to protect systems exists today, the major research thrust in computer communication security should lie in integrating this technology into existing and new applications. Lower cost personal identification technology must be investigated. We shall study cost-effective methods of implementing the needed security provisions, using the latest in computer, electronic and telephony technologies.

Many of the specialty fields of mathematics will be used to develop and evaluate cryptographic methods for assuring adequate integrity and security. Inexpensive methods for assuring the physical and electronic security of the devices implementing computer and telecommunication security will be investigated.

The payoff from this research will be reliable computer security for home banking, home voting or polling, electronic mail, home purchasing transactions. remote office operations and other emerging communications applications.

Let me close by quoting a manager of one of the Bureau's computer security programs, whose remarks appeared in a new magazine article on this subject. Dr. Stuart Katzke says:

> The owners of data banks that have never been penetrated are like people who have never been mugged. They say to themselves, "It can't happen to me." Well, computer owners are beginning to realize that it can happen to them and they're beginning to lock their electronic doors. But it's going to take some time before everybody gets the word.

We at NBS hope the word begins to spread more quickly. Thank you for asking us to appear today. Dr. Branstad and I will be happy to answer any questions you may have.

[The prepared statement of Mr. Lyons follows:]

STATEMENT OF
JOHN W. LYONS, ACTING DIRECTOR
NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
HEARINGS ON TELECOMMUNICATIONS SECURITY AND PRIVACY
OCTOBER 17, 1983

1. Introduction

I am John Lyons, Acting Director of the National Bureau of Standards (NBS). I am accompanied today by Dr. Dennis Branstad, Manager of the Computer Integrity and Security Technology Group in the Bureau's Institute for Computer Sciences and Technology (ICST). We are pleased to have this opportunity to testify before this Subcommittee on the important topics of computer communications security and privacy.

I would like to present an overview of the Institute's Computer Security and Risk Management Program which covers the subjects of computer communications security and privacy. I will then highlight the technology of computer network security being developed for reducing the vulnerabilities of computers and communications.

2. A Perspective on Computer Security and Privacy

Computer security is a complex area that involves numerous scientific disciplines and related management issues. Computer security has been discussed for nearly twenty years, but various publicized incidents have recently brought to the nation's attention the need for computer security, and especially telecommunications security.

Every organization which uses a computer, especially those providing remote access to the computer, should be acquainted with the vulnerabilities that were exploited in these incidents, and should then consider its own vulnerabilities and related risks. Following this procedure, generally called a risk analysis or risk assessment, the organization should select a set of safeguards for minimizing the overall risk. When selecting safeguards, an overall balance must be maintained among security, cost and residual risk.

3. Purpose and Scope of the NBS Activities in Computer Security and Privacy

NBS is the nation's central reference laboratory, providing measurement methods, standards, and data that are used throughout the government and industry. It is a technical organization that encourages and performs research, technological development and standards in many specific disciplines. NBS works with the technical leaders and managers throughout government and industry in performing its activities. The Institute for Computer Sciences and Technology, one of NBS's three major technical elements, has played a leading role in developing standards, guidelines and technical publications specifying cost-effective means for improving security in a variety of Federal and private sector applications where national security is not at stake. National security applications generally require more stringent safeguards

which are used on a case-by-case basis.
Computer security thus covers a spectrum of solutions which must be applied to a spectrum of problems. The problems range from accidental errors and omissions of people performing their authorized duties to high technology attacks on classified systems. The ICST program addresses the spectrum of problems and recommended solutions up to those related to classified computer systems. We feel that the administrative procedures and a majority of the technology comprising the common problem solutions are presently available. In certain areas implementation standards and guidelines are still needed even though the technology is available. Our program includes plans for performing research needed to solve several technical problems in specific application areas at the top of our problem spectrum. Our overall goal is to have a wide range of cost-effective solutions to be selected based on the results of a risk assessment. Automated solutions which are integrated into computers and terminals as standard features or standard options are desired in applying this needed technology.

I would like to specifically address the areas of interest detailed in your letter of invitation. I will outline our activities in computer and communications security; the generic vulnerabilities of computers and computer networks that are addressed by our technical activities; several areas of research necessary to support these activities; and some of the security technology being used in government and private sector applications.

3.1 General Computer Security Activities

To place our computer telecommunications security activities in context, I would like to present a synopsis of our range of computer security and risk management activities and then to focus on the telecommunications aspects. In each of the following areas of computer security, we have published, or are about to publish, documents containing technical information and related administration guidance for implementing and using this technology.

*RISK ASSESSMENT

Risk assessment is a procedure for estimating potential losses related to accidents or intentional misuse of ADP systems. The results of a risk assessment are used in selecting cost effective safeguards.

*CERTIFICATION AND ACCREDITATION

Certification is a procedure of evaluating the effectiveness of safeguards selected for a particular computer system. Accreditation is the process of approving the system for use.

*CONTINGENCY PLANNING

Contingency planning is the administrative preparation to assure continuity of ADP services should an unexpected event occur.

*SECURITY OF SMALL SYSTEMS

The widespread use of personal and professional computers and computer-based word processors has raised many questions regarding the security requirements and capabilities of small systems. We are investigating the security issues and technology of these systems.

*PERSONAL IDENTIFICATION

The fundamental requirement for controlling access to computer systems and networks is being able to accurately identify the authorized users. Over the past several years, we have investigated fingerprint readers, voice recognizers, automated human signature verifiers, hand geometry readers and palmprint readers. These devices rely on accurately differentiating among people based on a particular physical characteristic.

*PASSWORD USAGE

Passwords are the least expensive method of identifying computer users and, if properly implemented and used, provide a reasonable level of initial access control for a distributed computer system or network. We are completing a proposed standard on password usage which specifies ten factors and related security criteria that must be considered when designing and implementing a password system.

3.2 Specific Computer Communications Security Activities

The primary goal of the Institute's computer communications security activities is to encourage widespread availability of cost-effective telecommunications security technology for users throughout the government and private industry. Telecommunications security standards are necessary to assure that requested access from a terminal to a computer in any computer network is authorized, that the data being transmitted are not disclosed or modified without authorization, and that the terminal and the computer are mutually authenticated.

Our telecommunications security activities include developing standards for assuring the security and integrity of computer networks being developed for use by government and private sector organizations which do not process national security information. Standards for Federal use are issued by the Department of Commerce as Federal Information Processing Standards (FIPS). We are also participating in the American National Standards Institute (ANSI) activities to develop voluntary standards for use throughout private industry. ANSI standards are adopted as Federal standards when they satisfy Federal requirements. Compatible Federal and ANSI standards will reduce the cost of commercial equipment meeting the standards because of the increased customer base and will allow secure telecommunications between Federal and private ADP organizations.

The Bureau's Institute for Computer Sciences and Technology inititated a program in 1973 to establish a series of standards for assuring the integrity and security of computer networks. This cooperative program between government and industry has resulted in a number of activities that have resulted in Federal and ANSI compatible standards. The principal results of this program are:

*DATA ENCRYPTION STANDARD (DES)

In 1977, NBS published the Data Encryption Standard (DES) which specified a cryptographic algorithm for the protection of unclassified but sensitive computer data. This algorithm was developed in the private sector, submitted to the NBS in response to a public solicitation for such algorithms, and reviewed by the National Security Agency at the request of NBS.

The standard has been widely adopted, was published as ANSI standard X3.92-1981, and is recommended for use by the American Bankers Association for protecting electronic funds transfers.

*DES MODES OF OPERATION STANDARD

NBS published a FIPS on the Modes of Operation of the DES in 1980. This document specifies four modes of providing security to a variety of telecommunications applications, ranging from character oriented data transfer to protecting digital voice transmissions. ANSI published a standard specifying the same four modes of operation in 1983.

*DATA INTEGRITY STANDARD

Integrity is the assurance that data has not been modified, either accidentally or intentionally, without authorization. While integrity is important in all computer applications, it is especially important in financial transactions. A proposed Data Integrity Standard, scheduled for publication in 1984, can be used to put a cryptographic seal on data so that any unauthorized modification can be detected. The American Bankers Association, as Secretariat of ANSI activities on financial transactions, has published an ANSI standard for protecting the integrity of financial electronic funds transfers using this technique.

*OPEN SYSTEMS INTERCONNECTION (NETWORK) SECURITY

The open systems interconnection model of the International Organization of Standardization (ISO), is a conceptual architecture for communicating among a variety of information systems. The Institute has been active in ANSI activities developing integrity and security standards in this internationally accepted computer communications model.

*USER ACCESS AUTHORIZATION

Once the identity of an authorized user of a computer system has been established, the system should control the user's further access to data and resources of the system. A guideline on how to establish access authorization requirements and to implement the necessary access control mechanisms is presently being developed.

4. Computer Communications Security Vulnerabilities and Countermeasures

The information processing age has brought us to the point where great quantities of information must be available at many locations. The information must be current, accurate and easily accessible. Computer networks, which are integrated systems of computers and digital telecommunications, provide the desired access to information. Examples of large scale information networks include: airline reservation systems; stock market information systems; and credit card verification systems. Scaled-down information networks called "electronic bulletin boards" allow widespread sharing of information on special interest subjects. The trend towards distributed processing, marked by the entrance of micro-computers and end-user computing, has emphasized the need for computer network security.

The general security requirements of computer networks can be summarized as follows:

*Availability - Assuring that the network is available to provide the desired access;

*Controlled Accessibility - Assuring that the network provides access only to authorized users performing authorized tasks;

*Integrity - Protection of data from unauthorized modification, insertion, deletion, or destruction;

*Privacy (Secrecy) - Protection of data from unauthorized disclosure;

*Traffic flow security - Assuring that the identities of the communicating users, the quantity of data communicated, and the time and duration of communication are protected.

These security requirements are based on a number of generic vulnerabilites of computer and communications networks. I would like to outline some of these generic vulnerabilities and discuss the technology that is available or being developed to counter many of the common security problems identified in existing systems and networks.

The news media have recently carried numerous stories about young "computer hackers" gaining unauthorized access to computers throughout the country. Our review of these accounts leads us to believe that the vulnerabilities which allowed the unauthorized access were in the personal identification and access authorization sub-systems. Much of the needed technology already exists, and if properly applied, would have prevented the success of these unauthorized accesses. Our highest priority in our computer security activities is to transfer this technology to manufacturers if electronic equipment is needed, to software developers if computer program enhancements are needed, and to users.

The trend to distributed, "user friendly" computer capability has posed new problems for ADP managers. Telephone numbers which provide remote electronic access to computers are often published (e.g., for public "electronic bulletin boards"). Even unpublished computer telephone numbers can be "guessed" with known probability (1/10,000 if the exchange of the computer is known) or can be electronically searched (as depicted in the movie "Wargames"). The technology exists to have the "called" computer request the identification of the "calling" party, verify that this party is on the approved access list, break the original connection, and then call back to the correct location of the acceptable authorized user. Thus, a person attempting to "masquerade" as an authorized user (from an unauthorized location) can be prevented from gaining even initial access to the computer.

Once initial access to the computer is gained, only a "password" generally stands between the user and access to the system. Password systems, while potentially capable of providing good security in many applications, are vulnerable to many failures of human nature in users and managers. Commercial computer systems are generally delivered with an initial set of "default" passwords which are used by the system's operators and maintenance personnel. These "default" passwords are often not deleted or changed to locally generated passwords following installation. The local system is then vulnerable to easy access by anyone who has purchased an identical system or knows the easily remembered "default" passwords.

Users often select passwords that are too short or are associated with something personal about the user (for ease of memorization). Sometimes the passwords are "memorized" by writing the password on a piece of paper and attaching the password to the terminal. NBS has published several documents on how to use password systems effectively and we are completing a Federal Information Processing Standard on Password Usage. This proposed standard requires specific security criteria to be met in all Federal ADP installations and suggests many ways that the system can provide automated methods of good password control. We believe that the specific vulnerabilities of password systems that were depicted in "Wargames" (i.e., using the name of a relative as a password and hiding a password in a "secret" location) and in the stories about "computer hackers" (i.e., not changing passwords following system installation) could not have been exploited if the technical and management provisions specified in the proposed Password Usage Standard had been followed.

If electronic access to the computer and access to the system are initially achieved, few systems have additional security provisions to monitor and control the activity of the user. The User Access Authorization guideline presently being completed discusses some of the needed access control provisions.

The following generic vulnerabilities of computers and communications networks must be countered:

*Browsing - unauthorized reading of data available to authorized users of the system;

*Unauthorized modification, destruction, insertion or deletion of data;

*Passive "wiretapping" - unauthorized reading of data during transmission;

*Active "wiretapping" - unauthorized modification of data during transmission;

*Control signal logging - unauthorized recording of the dial pulses or tones of telephone networks;

*"Piggy backing" - attaching a terminal of an unauthorized user to a communications connection being used by an authorized user;

*"Spoofing" - an unauthorized user or device pretending to be an authorized user or device.

Proper use of the Data Encryption Standard, the standard Modes of Operation of the DES, and a good cryptographic key management system will prevent the success of any attempt to exploit these generic vulnerabilities of computer networks.

5. Research in Computer and Communications Security

While much of the technology needed to protect systems exists today, the major research thrust in computer communications security should lie in integrating this security technology into existing and newly emerging applications areas such as:

*Network integrity and security in the ISO layered communications architecture;

*Cryptographic key management in computer telecommunications networks;

*Improved methods of personal identification for controlling access to computer networks;

*Integrity/security architectures of personal computers;

*Integrity/security protocols of transactions initiated from home telephones or home computers;

*Methods for generating digital "signatures" on electronic messages, contracts, etc.;

*Methods for providing security to voice initiated computer transactions and to computer generated voice responses;

*Assessment of traffic flow security/privacy procedures on computer telecommunications networks.

Many computer communications applications being developed could utilize the results of research in these areas. They include:

*Home banking
*Home voting/polling
*Electronic mail: voice and data
*Home initiated purchasing transactions
*Electronic contract negotiation
*Digital signature notarization of contracts
*Remote office operation
*Computer software copyright protection

Research in the above areas will involve several technical disciplines. Personal identification technology must be investigated to determine what characteristics can be easily determined to distinguish one person from another. Computer, electronic and telephony technologies must be used in developing cost-effective methods of implementing the needed security provisions. Many of the specialty fields of mathematics must be used to develop and evaluate cryptographic methods for assuring adequate integrity and security. Inexpensive methods for assuring physical and electronic security for the devices implementing computer and telecommunications security must be investigated.

6. Opportunities for Leadership in Computer and Communications Security

ICST has played a significant leadership role in the development of computer security technology, management procedures, standards and guidelines. The thrust of this role has been through the Federal and ANSI standards development activities. To support these standards development activities, the Institute has performed applied research and development in computer security technology, identified generic requirements for computer security, prepared technical specifications of proposed standards and assisted various organizations in utilizing the standards after adoption.

We have served a technology transfer role between the public and private sectors. Our activities include identifying the needs for security technology by both industry and Federal computer users and then stimulating the sharing of technical information among these users. We sponsor, or participate in, numerous conferences, workshops and meetings on computer security. We encourage the development and use of off-the-shelf automated solutions to security problems when such solutions are known and cost-effective. We develop standards through participation in, and leadership of, voluntary industry standards activities.

NBS works closely with other Federal organizations, both in developing security technology and in transfering the technology. We have worked with the National Security Agency in developing computer communications security standards. We have assisted the

DOD Computer Security Center in transferring "Trusted System" technology to users in government and the private sector. We have participated with the National Communications System and the General Services Administration in developing Federal Standards for Telecommunications. We have provided technical inputs to the Office of Management and Budget on its Circular A-71, Transmittal Memorandum Number 1. We have cosponsored several workshops on computer security evaluation with the General Accounting Office. We have presented computer security conferences with the Department of Defense, the Office of Personnel Management, the Department of Agriculture and the Federal ADP Users Group. Many lectures on computer security have been given at the DOD Computer Institute and at meetings sponsored by the Department of Energy, Department of Health and Human Services and at the National Aeronautical and Space Administration.

7. Summary

I have summarized only the highlights of the computer and communications security activities at the National Bureau of Standards, concentrating on the activities specified in your letter of invitation to appear before this Subcommittee. I have mentioned our relationships with some of the Federal organizations having a lead role in computer security. We also work very closely with private industry and state governments in need of the technology and information we have available.

Thank you for inviting us to appear before you. We will be happy to answer any questions at this time.

JOHN W. LYONS

Date of Birth: November 5, 1930

Birthplace: Reading, Massachusetts

Education: Degrees

Harvard University, A.B., Chemistry
1952
Washington University, A.M., Physical Chemistry
1963
Washington University, Ph.D., Physical Chemistry
1964

Positions:

Acting Deputy Director
National Bureau of Standards

Dr. Lyons was appointed in April 1983 as Acting Deputy Director of the National Bureau of Standards. In this position, Dr. Lyons is responsible for the efficient execution of the Bureau's operational programs. He coordinates, monitors, and assesses progress of all NBS technical projects, and of the supporting services.

(NBS is the Nation's central reference laboratory, providing measurement methods, standards, and data that are used in industry, commerce, government, and universities. Bureau headquarters are located in Gaithersburg, Maryland, with a second laboratory at Boulder, Colorado. Total staff numbers about 3,200).

As Director of the National Engineering Laboratory from December 1977 until April 1983, Dr. Lyons was responsible for NBS's research in applied mathematics, building technology, electronics and electrical engineering, energy conservation, engineering standards development, fire, manufacturing engineering and chemical engineering.

Dr. Lyons was Director of the NBS Center for Fire Research until December 18, 1977, and was responsible for providing scientific and technical knowledge applicable to the prevention and control of fires.

Dr. Lyons served in various research and development positions at the Monsanto Company from 1955 to 1973. He specialized in the chemistry and uses of phosphorus-based chemicals including fire retardants. He served from 1971 to 1973 as a member of the ad hoc panel of fire research, a National Academy of Sciences evaluation panel for the National Bureau of Standards.

Dr. Lyons is author of two books: Viscosity and Flow Measurements and The Chemistry and Uses of Fire Retardants. He has contributed chapters to five other books and has written numerous papers and articles on technical or research topics. His early research interest was the physical chemistry of polyelectrolyte solutions, especially formation of complexes with metal ions. This work emphasized the behavior of inorganic polyphosphates and desoxy ribonucleic acid (DNA).

Dr. Lyons is a Fellow of the American Association for the Advancement of Science, Fellow of the Washington Academy of Science, member of the American Chemical Society (past chairman of the St. Louis Section), member of the American Institute of Chemical Engineers and member of Sigma Xi. He serves on the Advisory Committee for Engineering, National Science Foundation; Advisory Council, College of Engineering, University of Maryland; Board of Directors, National Fire Protection Association. He is serving on a special committee of the Maryland State Board for Higher Education to study the needs for engineering education. He was chairman of the Products Research Committee (1974-1979), a nine-member charitable trust administering a $5M research fund on fire research; co-chairman of the US-Japan Natural Resources Panel of Fire Research (1975-1978). He received the Presidential Management Improvement Award in 1977 and the U.S. Department of Commerce Gold Medal, also in 1977. In 1981 he received the Presidential Rank Award of Distinguish Executive.

4/20/83

Mr. GLICKMAN. Thank you for your excellent and, I think, important technical testimony that is necessary. Your entire statement provides some information which will be useful when we make our recommendations.

How large is your effort, in terms of people and money, on computer security issues and technology?

Mr. LYONS. We have seven full-time in this effort and half a million dollars.

Mr. GLICKMAN. I'm sorry, I didn't hear the last.

Mr. LYONS. Half a million dollars.

Mr. GLICKMAN. Half a million dollars. Has it been roughly stable or is it increased?

Mr. LYONS. Roughly stable over the years.

Mr. GLICKMAN. What is the life span of DES, the data encryption standard, and will new computers make it obsolete?

Mr. LYONS. Well, we've just verified it for another 5 years in a Federal Register notice. It's not clear that the basic algorithm will have to be changed in the future, but we are monitoring that.

Mr. GLICKMAN. When you say, "It's not clear," what do you mean, "It's not clear"?

Mr. LYONS. Well, I'd ask Dr. Branstad to go into detail.

Mr. BRANSTAD. OK. One of the things that we've been doing——

Mr. GLICKMAN. Push your——

Mr. BRANSTAD. Push to talk.

Mr. GLICKMAN. Yeah.

Mr. BRANSTAD. One of the things that we've been doing is continually to monitor the different applications of the DES and the state of technology with respect to the security provided by DES. We evaluated it. It has been just confirmed as being very adequate for all commercial applications we intended it for for the next 5 years and I don't see any changes that are going to be needed to the DES standard whatsoever, based on any of the emerging computers.

Mr. GLICKMAN. OK. There are a number of—I asked the same question of the previous witness from the GAO, but there are a number—well, similar question—but there are a number of devices and packages that utilize the DES standard. A recent article noted that DES packages are not "hot sellers."

Can you explain why these are not being used? Why do managers tend to ignore the problem?

Mr. Lyons. I think that's a lack of knowledge and understanding of the problem primarily. There is a cost involved with installing DES. First of all, the $250. You have to get these chips, which don't cost $250, but the system does. For some small systems, that may be a barrier.

If they don't feel that it's worth it; if they don't feel that they're losing that much, then they may decide they don't want to go after it. There are other lower level solutions, of course; adequate passwords, for example, are much less expensive.

I think it's, though, a lack of sensitivity to the growing problem more than anything else. This is not an expensive technology——

Mr. Glickman. Yes.

Mr. Lyons [continuing]. Especially if you buy it and ship, rather than——

Mr. Glickman. And compared to the loss that could result, it could be infinitesimal in terms of——

Mr. Lyons. Yes.

Mr. Glickman. I just think a lot of folks don't know that there is some current technology which will provide them protection. It may not be absolute and it may be——

Mr. Lyons. Well, they may think that encryption is a terribly sophisticated business, and it is in one sense, but in terms of the cost, it is not.

Mr. Glickman. Yes.

Should NBS—should the NBS role in computer security be expanded to meet the growing needs of the nondefense sector and what encouragement should be given to promoting exchanges of information on this subject?

Mr. Lyons. Well, I think the program that we have has proven over the years to be adequate. We feel that we're on top of this field and I don't see that the technical work at the Bureau needs any particular change. I'm confident that the group is doing the job that should be done.

I think that what does need more attention is that the ADP managers need to respond to the information that we have provided. We have had workshops, as I show in these documents. We've been doing as much as we can on technology transfer, but there needs to be more receptivity on the other end. So we'll keep holding workshops and we hope more and more people will come.

Mr. Glickman. Going back to DES for a minute, are any agencies in government using DES?

Mr. Branstad. Yes. I have worked, I guess, over about the last 6 years with many different agencies as they first address their computer security problems, first address the management issues which are the first things to address. Then when they finally get to the level of sophistication and need, where they've identified the need for DES, they are starting to do it.

Several agencies are using it for terminal-to-computer telecommunication security for authenticating the two ends of the device and many other applications.

Mr. Glickman. Do you know off your head which agencies are using it?

Mr. Branstad. I can give you examples of several: Drug Enforcement Agency is interested in protecting the information that's being transmitted in that area; the Social Security Administration has called me several times, asking for help and guidance in implementing it and using it; there are several hundred thousands of applications identified in the unclassified, nondefense-related DOD area.

Mr. GLICKMAN. OK.

Let me just ask you one final question. Would it be practical or desirable to institute a system of classifying nonnational security information in the Government?

Mr. LYONS. Well, as has been testified to earlier, there have been attempts to do that. There hasn't been a consensus reached. Some of the data naturally falls into these categories, for example, the Privacy Act, which was mentioned. The Freedom of Information Act defines proprietary information, that is, certain information that agencies may withhold.

Then there's fiscal information which is a fairly separate category. Then there's information that we really want everybody to have. So I can think of, off the top of my head, at least those categories which would probably further subdivide.

I think it could be done. It's a policy decision. I think OMB will have to consider whether they want to require the Federal Government to develop that consensus. We could be helpful. We can't do it.

Mr. GLICKMAN. OK. Thank you very much for your testimony today.

Our next witness is Melville H. Klein, Director of the DOD Computer Security Center at the National Security Agency, and I think you may be accompanied by some people and you may want to identify them for the record.

Mr. Klein, we appreciate your coming here. We understand this is one of the first times NSA has come down and testified on this subject and so we are most appreciative and you may either read your statement or summarize it. It doesn't look too long, but it's up to you.

STATEMENT OF MELVILLE H. KLEIN, DIRECTOR, DOD COMPUTER SECURITY CENTER, NATIONAL SECURITY AGENCY, U.S. DEPARTMENT OF DEFENSE; ACCOMPANIED BY COL. ROGER R. SCHELL, DEPUTY DIRECTOR, DOD COMPUTER SECURITY CENTER

Mr. KLEIN. Mr. Chairman, I'm pleased to be here today to represent the Director of NSA. I'm Melville Klein, Director of the DOD Computer Security Center, and with me is my Deputy, Colonel Roger Schell, U.S. Air Force.

I have submitted a statement and I would just like to highlight some of the points in that statement and then be available for any questions that you might have.

Today I'd like to address NSA research activities that are relevant to your examination of security and privacy in the civil community.

We find that unclassified aspects of computer security, many of which are developed at NSA, are very applicable to the problems being addressed by the civil community and the Federal sector of the U.S. Government.

The ingredients of electronic information security are the following: cryptographic security for the external communications, personnel security for people who handle sensitive classified information, physical security for the facilities in which these operations are conducted, procedural security, administrative controls, emanation security and the subject that I'm going to address this morning, computer security.

There's a great diversity of opinion among the experts for the recipe needed to address the threats facing the civil community in how much of varying—these varying ingredients have to be applied. I believe there's a great deal of commonality between the defense sector and the civil community, in both the vulnerabilities we face and the kind of measures we would want to apply to address the threats.

The three areas that I think are common to each sector that have been addressed this morning are access controls, labeling of information—I think that you've asked each of the previous witnesses the need to classify information in the nonsecurity-related information—and last—I'm talking about labeling information electronic form—and last, secure auditing capability.

Over the past decade, the interest in information protection and privacy has spread with the rapid and pervasive use of computers in almost every facet of our everyday lives. Efforts to counter the threats to privacy of citizens and the confidentiality of business and nonnational security Government information have been undertaken by the private sector and by civil agencies, as you've heard from the previous witness.

I would like to address how these activities have, and can continue to benefit from the communication security and computer security research programs at NSA. I will first review the origin and purpose and operations of the DOD Computer Security Center.

It is an outgrowth of initiatives taken in the late 1970's under the auspices of the Assistant Secretary of Defense for Command Control and Intelligence to coordinate ongoing computer security research within the Department. In January of 1981, the Secretary of Defense assigned to the Director of NSA certain responsibilities for computer security within the DOD.

The Center began operation in June of 18—1981 as a separate and unique entity within NSA for this purpose. At that time, a cadre of 31 people and the budgets that existed within NSA, related to computer security, were put into practice under this new organization.

The implementing directive establishing the Center formally was issued in October of 1982 by the Office of the Secretary of Defense. The Center has a five-pronged mission: First is to develop and promulgate uniform computer security criterion standards that will lead to widespread availability of trusted products from computer vendors. These standards have been developed and issued and they were developed in an ecumenical way with participation by members of the civil agencies, computer industry, and the academic community.

I have a copy of the computer criteria that I would be pleased to leave with you today. It's titled, "The Computer Security Evaluation Criteria."

[The Department of Defense criteria follows:]

CSC-STD-001-83
Library No. S225,711

DEPARTMENT OF DEFENSE
TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

15 August 1983

CSC-STD-001-83

FOREWORD

This publication, "Department of Defense Trusted Computer System Evaluation Criteria," is being issued by the DoD Computer Security Center under the authority and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The criteria defined in this document constitute a uniform set of basic requirements and evaluation classes for assessing the effectiveness of security controls built into Automatic Data Processing (ADP) systems. These criteria are intended for use in the evaluation and selection of ADP systems being considered for the processing and/or storage and retrieval of sensitive or classified information by the Department of Defense. Point of contact concerning this publication is the Office of Standards and Products, Attention: Chief, Computer Security Standards.

Melville H Klein

Melville H. Klein
Director
DoD Computer Security Center

15 August 1983

ACKNOWLEDGMENTS

Special recognition is extended to Sheila L. Brand, DoD Computer Security Center (DoDCSC), who integrated theory, policy, and practice into and directed the production of this document.

Acknowledgment is also given for the contributions of: Grace Hammonds and Peter S. Tasker, the MITRE Corp., Daniel J. Edwards, Col. Roger R. Schell, Marvin Schaefer, DoDCSC, and Theodore M. P. Lee, Sperry UNIVAC, who as original architects formulated and articulated the technical issues and solutions presented in this document; Jeff Makey and Warren F. Shadle, DoDCSC, who assisted in the preparation of this document; James P. Anderson, James P. Anderson & Co., Steven B. Lipner, Digital Equipment Corp., Clark Wiessman, System Development Corp., LTC Lawrence A. Noble, formerly U.S. Air Force, Stephen T. Walker, formerly DoD, Eugene V. Epperly, DoD, and James E. Studer, formerly Dept. of the Army, who gave generously of their time and expertise in the review and critique of this document; and finally, thanks are given to the computer industry and others interested in trusted computing for their enthusiastic advice and assistance throughout this effort.

PREFACE

The trusted computer system evaluation criteria defined in this document classify systems into four broad hierarchical divisions of enhanced security protection. They provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products. The criteria were developed with three objectives in mind: (a) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information; (b) to provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications; and (c) to provide a basis for specifying security requirements in acquisition specifications. Two types of requirements are delineated for secure processing: (a) specific security feature requirements and (b) assurance requirements. Some of the latter requirements enable evaluation personnel to determine if the required features are present and functioning as intended. Though the criteria are application-independent, it is recognized that the specific security feature requirements may have to be interpreted when applying the criteria to specific applications or other special processing environments. The underlying assurance requirements can be applied across the entire spectrum of ADP system or application processing environments without special interpretation.

INTRODUCTION

Historical Perspective

In October 1967, a task force was assembled under the auspices of the Defense Science Board to address computer security safeguards that would protect classified information in remote-access, resource-sharing computer systems. The Task Force report, "Security Controls for Computer Systems," published in February 1970, made a number of policy and technical recommendations on actions to be taken to reduce the threat of compromise of classified information processed on remote-access computer systems.[33] Department of Defense Directive 5200.28 and its accompanying manual DoD 5200.28-M, published in 1972 and 1973 respectivley, responded to one of these recommendations by establishing uniform DoD policy, security requirements, administrative controls, and technical measures to protect classified information processed by DoD computer systems.[8;9] Research and development work undertaken by the Air Force, Advanced Research Projects Agency, and other defense agencies in the early and mid 70's developed and demonstrated solution approaches for the technical problems associated with controlling the flow of information in resource and information sharing computer systems.[1] The DoD Computer Security Initiative was started in 1977 under the auspices of the Under Secretary of Defense for Research and Engineering to focus DoD efforts addressing computer security issues.[32]

Concurrent with DoD efforts to address computer security issues, work was begun under the leadership of the National Bureau of Standards (NBS) to define problems and solutions for building, evaluating, and auditing secure computer systems.[17] As part of this work NBS held two invitational workshops on the subject of audit and evaluation of computer security.[19;27] The first was held in March 1977, and the second in November of 1978. One of the products of the second workshop was a definitive paper on the problems related to providing criteria for the evaluation of technical computer security effectiveness.[19] As an outgrowth of recommendations from this report, and in support of the DoD Computer Security Initiative, the MITRE Corporation began work on a set of computer security evaluation criteria that could be used to assess the degree of trust one could place in a computer system to protect classified data.[23;24;30] The preliminary concepts for computer security evaluation were defined and expanded upon at invitational workshops and symposia whose participants represented computer security expertise drawn from industry and academia in addition to the government. Their work has since been subjected to much peer review and constructive technical criticism from the DoD, industrial research and development organizations, universities, and computer manufacturers.

The DoD Computer Security Center (the Center) was formed in January 1981 to staff and expand on the work started by the DoD Computer Security Initiative.[15] A major goal of the Center as given in its DoD Charter is to encourage the widespread availability of trusted computer systems for use by those who process classified or other sensitive information.[10] The criteria presented in this document have evolved from the earlier NBS and MITRE evaluation material.

Scope

The trusted computer system evaluation criteria defined in this document apply to both trusted general-purpose and trusted embedded (e.g., those dedicated to a specific application) automatic data processing (ADP) systems. Included are two distinct sets of requirements: 1) specific security feature requirements; and 2) assurance requirements. The specific feature requirements encompass the capabilities typically found in information processing systems employing general-purpose operating systems that are distinct from the applications programs being supported. The assurance requirements, on the other hand, apply to systems that cover the full range of computing environments from dedicated controllers to full range multilevel secure resource sharing systems.

Purpose

As outlined in the Preface, the criteria have been developed for a number of reasons:

- To provide users with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.

- To provide guidance to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements for sensitive applications.

- To provide a basis for specifying security requirements in acquisition specifications.

With respect to the first purpose for development of the criteria, i.e., providing users with a security evaluation metric, evaluations can be delineated into two types: (a) an evaluation can be performed on a computer product from a perspective that excludes the application environment; or, (b) it can be done to assess whether appropriate security measures have been taken to permit the system to be used operationally in a specific environment. The former type of evaluation is done by the Computer Security Center through the Commercial Product Evaluation Process. That process is described in Appendix A.

The latter type of evaluation, i.e., those done for the purpose of assessing a system's security attributes with respect to a specific operational mission, is known as a certification evaluation. It must be understood that the completion of a formal product evaluation does not constitute certification or accreditation for the system to be used in any specific application environment. On the contrary, the evaluation report only provides a trusted computer system's evaluation rating along with supporting data describing the product system's strengths and weaknesses from a computer security point of view. The system security certification and the formal approval/accreditation procedure, done in accordance with the applicable policies of the issuing agencies, must still be followed before a system can be approved for use in processing or handling classified information.[8;9]

The trusted computer system evaluation criteria will be used directly and indirectly in the certification process. Along with applicable policy, it will be used directly as the basis for evaluation of the total system and for specifying system security and certification requirements for new acquisitions. Where a system being evaluated for certification employs a product that has undergone a Commercial Product Evaluation, reports from that process will be used as input to the certification evaluation. Technical data will be furnished to designers, evaluators and the Designated Approving Authorities to support their needs for making decisions.

Fundamental Computer Security Requirements

Any discussion of computer security necessarily starts from a statement of requirements, i.e., what it really means to call a computer system "secure." In general, secure systems will control, through use of specific security features, **access to information** such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information. Six fundamental requirements are derived from this basic statement of objective: four deal with what needs to be provided to control access to information; and two deal with how one can obtain credible assurances that this is accomplished in a trusted computer system.

POLICY

Requirement 1 - SECURITY POLICY - There must be an explicit and well-defined security policy enforced by

the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object. Computer systems of interest must enforce a mandatory security policy that can effectively implement access rules for handling sensitive (e.g., classified) information.[7] These rules include requirements such as: No person lacking proper personnel security clearance shall obtain access to classified information. In addition, discretionary security controls are required to ensure that only selected users or groups of users may obtain access to data (e.g., based on a need-to-know).

Requirement 2 - MARKING - Access control labels must be associated with objects. In order to control access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity level (e.g., classification), and/or the modes of access accorded those subjects who may potentially access the object.

ACCOUNTABILITY

Requirement 3 - IDENTIFICATION - Individual subjects must be identified. Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with. This identification and authorization information must be securely maintained by the computer system and be associated with every active element that performs some security-relevant action in the system.

Requirement 4 - ACCOUNTABILITY - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party. A trusted system must be able to record the occurrences of security-relevant events in an audit log. The capability to select the audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis. Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations.

ASSURANCE

Requirement 5 - ASSURANCE - The computer system must contain hardware/software mechanisms that can be

independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above. In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions. These mechanisms are typically embedded in the operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such system mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency.

Requirement 6 - CONTINUOUS PROTECTION - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes. No computer system can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion. The continuous protection requirement has direct implications throughout the computer system's life-cycle.

These fundamental requirements form the basis for the individual evaluation criteria applicable for each evaluation division and class. The interested reader is referred to Section 5 of this document, "Control Objectives for Trusted Computer Systems," for a more complete discussion and further amplification of these fundamental requirements as they apply to general-purpose information processing systems and to Section 7 for amplification of the relationship between Policy and these requirements.

Structure of the Document

The remainder of this document is divided into two parts, four appendices, and a glossary. Part I (Sections 1 through 4) presents the detailed criteria derived from the fundamental requirements described above and relevant to the rationale and policy excerpts contained in Part II.

Part II (Sections 5 through 10) provides a discussion of basic objectives, rationale, and national policy behind the development of the criteria, and guidelines for developers pertaining to: mandatory access control rules implementation, the covert channel problem, and security testing. It is divided into six sections. Section 5 discusses the use of control objectives in general and presents the three basic control objectives of the criteria. Section 6 provides the theoretical basis behind the criteria.

Section 7 gives excerpts from pertinent regulations, directives, OMB Circulars, and Executive Orders which provide the basis for many trust requirements for processing nationally sensitive and classified information with computer systems. Section 8 provides guidance to system developers on expectations in dealing with the covert channel problem. Section 9 provides guidelines dealing with mandatory security. Section 10 provides guidelines for security testing. There are four appendices, including a description of the Trusted Computer System Commercial Products Evaluation Process (Appendix A), summaries of the evaluation divisions (Appendix B) and classes (Appendix C), and finally a directory of requirements ordered alphabetically. In addition, there is a glossary.

Structure of the Criteria

The criteria are divided into four divisions: D, C, B, and A ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the most comprehensive security. Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information. Within divisions C and B there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess. Assurance of correct and complete design and implementation for these systems is gained mostly through testing of the security-relevant portions of the system. The security-relevant portions of a system are referred to throughout this document as the Trusted Computing Base (TCB). Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. Increased assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous analysis during the design process.

Within each class, four major sets of criteria are addressed. The first three represent features necessary to satisfy the broad control objectives of Security Policy, Accountability, and Assurance that are discussed in Part II, Section 5. The fourth set, Documentation, describes the type of written evidence in the form of user guides, manuals, and the test and design documentation required for each class.

A reader using this publication for the first time may find it helpful to first read Part II, before continuing on with Part I.

PART I: THE CRITERIA

Highlighting is used in Part I to indicate criteria not contained in a lower class or changes and additions to already defined criteria. Where there is no highlighting, requirements have been carried over from lower classes without addition or modification.

1.0 DIVISION D: MINIMAL PROTECTION

This division contains only one class. It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

2.0 DIVISION C: DISCRETIONARY PROTECTION

Classes in this division provide for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.

2.1 CLASS (C1): DISCRETIONARY SECURITY PROTECTION

The Trusted Computing Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity. The following are minimal requirements for systems assigned a class (C1) rating:

2.1.1 SECURITY POLICY

2.1.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both.

2.1.2 ACCOUNTABILITY

2.1.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user.

2.1.3 ASSURANCE

2.1.3.1 Operational Assurance

2.1.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

2.1.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

2.1.3.2 Life-Cycle Assurance

2.1.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. (See the Security Testing guidelines.)

2.1.4 DOCUMENTATION

2.1.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

2.1.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

2.1.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing.

2.1.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

2.2 CLASS (C2): CONTROLLED ACCESS PROTECTION

Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation. The following are minimal requirements for systems assigned a class (C2) rating:

2.2.1 SECURITY POLICY

2.2.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both. **The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.**

2.2.1.2 Object Reuse

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

2.2.2 ACCOUNTABILITY

2.2.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. **The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.**

2.2.2.2 Audit

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

2.2.3 ASSURANCE

2.2.3.1 Operational Assurance

2.2.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

2.2.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

2.2.3.2 Life-Cycle Assurance

2.2.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. **Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.** (See the Security Testing guidelines.)

2.2.4 DOCUMENTATION

2.2.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

2.2.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. **The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.**

2.2.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing.

2.2.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

3.0 DIVISION B: MANDATORY PROTECTION

The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

3.1 CLASS (B1): LABELED SECURITY PROTECTION

Class (B1) systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed. The following are minimal requirements for systems assigned a class (B1) rating:

3.1.1 SECURITY POLICY

3.1.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

3.1.1.2 Object Reuse

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

3.1.1.3 Labels

Sensitivity labels associated with each subject and storage object under its control (e.g., process, file, segment, device) shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

3.1.1.3.1 Label Integrity

Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

3.1.1.3.2 Exportation of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the current security level associated with a single-level communication channel or I/O device.

3.1.1.3.2.1 Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

3.1.1.3.2.2 Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

3.1.1.3.2.3 Labeling Human-Readable Output

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable. paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

3.1.1.4 Mandatory Access Control

The TCB shall enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between subjects and objects controlled by the TCB: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the

---

* The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

3.1.2 ACCOUNTABILITY

3.1.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall **maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate** the user's identity **and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual user.** The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

3.1.2.2 Audit

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. **The TCB shall also be able to audit any override of human-readable output markings.** For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object **and the object's security level.** The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity **and/or object security level.**

3.1.3 ASSURANCE

3.1.3.1 Operational Assurance

3.1.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. **The TCB shall maintain process isolation through the provision of distinct address spaces under its control.** The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

3.1.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

3.1.3.2 Life-Cycle Assurance

3.1.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able

to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. All discovered flaws shall be removed or neutralized and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. (See the Security Testing Guidelines.)

3.1.3.2.2 Design Specification and Verification

An informal or formal model of the security policy supported by the TCB shall be maintained that is shown to be consistent with its axioms.

3.1.4 DOCUMENTATION

3.1.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

3.1.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. **The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner.**

3.1.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing.

3.1.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described. **An informal or formal description of the security policy model enforced by the TCB shall be available and an explanation provided to show that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model.**

Class (B1)

3.2 CLASS (B2): STRUCTURED PROTECTION

In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non-protection-critical elements. The TCB interface is well-defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration. The following are minimal requirements for systems assigned a class (B2) rating:

3.2.1 SECURITY POLICY

3.2.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

3.2.1.2 Object Reuse

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

3.2.1.3 Labels

Sensitivity labels associated with each **ADP system resource (e.g., subject, storage object) that is directly or indirectly accessible by subjects external to the TCB** shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

3.2.1.3.1 Label Integrity

Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

3.2.1.3.2 Exportation of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the current security level associated with a single-level communication channel or I/O device.

3.2.1.3.2.1 Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

3.2.1.3.2.2 Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

3.2.1.3.2.3 Labeling Human-Readable Output

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

3.2.1.3.3 Subject Sensitivity Labels

The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

3.2.1.3.4 Device Labels

The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be

---

* The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

3.2.1.4 Mandatory Access Control

The TCB shall enforce a mandatory access control policy over all **resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB.** These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between **all subjects external to the TCB and all objects directly or indirectly accessible by these subjects:** A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

3.2.2 ACCOUNTABILITY

3.2.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual user. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

3.2.2.1.1 Trusted Path

The TCB shall support a trusted communication path between itself and user for initial login and authentication. Communications via this path shall be initiated exclusively by a user.

3.2.2.2 Audit

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. **The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels.**

3.2.3 ASSURANCE

3.2.3.1 Operational Assurance

3.2.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified.

3.2.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

3.2.3.1.3 Covert Channel Analysis

The system developer shall conduct a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.)

3.2.3.1.4 Trusted Facility Management

The TCB shall support separate operator and administrator functions.

3.2.3.2 Life-Cycle Assurance

3.2.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. **The TCB shall be found relatively resistant to penetration.** All discovered flaws shall be **corrected** and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. **Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification.** (See the Security Testing Guidelines.)

3.2.3.2.2 Design Specification and Verification

A formal model of the security policy supported by the TCB shall be maintained that is **proven** consistent with its axioms. **A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface.**

3.2.3.2.3 Configuration Management

During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

3.2.4 DOCUMENTATION

3.2.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

3.2.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. **The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described.**

3.2.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing. **It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths.**

3.2.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of the security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamperproof, cannot be bypassed, and is correctly implemented. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.)

Class (B2)

3.3 CLASS (B3): SECURITY DOMAINS

The class (B3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration. The following are minimal requirements for systems assigned a class (B3) rating:

3.3.1 SECURITY POLICY

3.3.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (**e.g., access control lists**) shall allow users to specify and control sharing of those **objects**. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of **specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given.** Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

3.3.1.2 Object Reuse

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

3.3.1.3 Labels

Sensitivity labels associated with each ADP system resource (e.g., subject, storage object) that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

3.3.1.3.1 Label Integrity

Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

3.3.1.3.2 Exportation of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the current security level associated with a single-level communication channel or I/O device.

3.3.1.3.2.1 Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

3.3.1.3.2.2 Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

3.3.1.3.2.3 Labeling Human-Readable Output

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

3.3.1.3.3 Subject Sensitivity Labels

The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

3.3.1.3.4 Device Labels

The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

---

* The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

3.3.1.4 Mandatory Access Control

The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

3.3.2 ACCOUNTABILITY

3.3.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual user. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

3.3.2.1.1 Trusted Path

The TCB shall support a trusted communication path between itself and **users for use when a positive TCB-to-user connection is required (e.g., login, change subject security level).** Communications via this **trusted** path shall be **activated** exclusively by a user **or the TCB and shall be logically isolated and unmistakably distinguishable from other paths.**

3.3.2.2 Audit

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels. **The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded.**

3.3.3 ASSURANCE

3.3.3.1 Operational Assurance

3.3.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. **The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.**

3.3.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

3.3.3.1.3 Covert Channel Analysis

The system developer shall conduct a thorough search for **covert channels** and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.)

3.3.3.1.4 Trusted Facility Management

The TCB shall support separate operator and administrator functions. **The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.**

3.3.3.1.5 Trusted Recovery

Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.

3.3.3.2 Life-Cycle Assurance

3.3.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be **found resistant** to penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification. (See the Security Testing Guidelines.) **No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain.**

3.3.3.2.2 Design Specification and Verification

A formal model of the security policy supported by the TCB shall be maintained that is proven consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface. **A convincing argument shall be given that the DTLS is consistent with the model.**

3.3.3.2.3 Configuration Management

During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

3.3.4 DOCUMENTATION

3.3.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

3.3.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described. **It shall include the procedures to ensure that the system is initially started in a secure manner. Procedures shall also be included to resume secure system operation after any lapse in system operation.**

3.3.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths.

3.3.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of the security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamperproof, cannot be bypassed, and is correctly implemented. **The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the DTLS. The elements of the DTLS shall be shown, using informal techniques, to correspond to the elements of the TCB.** Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.)

Class (B3)

4.0 DIVISION A: VERIFIED PROTECTION

This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation.

4.1 CLASS (A1): VERIFIED DESIGN

Systems in class (A1) are functionally equivalent to those in class (B3) in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. Independent of the particular specification language or verification system used, there are five important criteria for class (A1) design verification:

- A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.
- An FTLS must be produced that includes abstract definitions of the functions the TCB performs and of the hardware and/or firmware mechanisms that are used to support separate execution domains.
- The FTLS of the TCB must be shown to be consistent with the model by formal techniques where possible (i.e., where verification tools exist) and informal ones otherwise.
- The TCB implementation (i.e., in hardware, firmware, and software) must be informally shown to be consistent with the FTLS. The elements of the FTLS must be shown, using informal techniques, to correspond to the elements of the TCB. The FTLS must express the unified protection mechanism required to satisfy the security policy, and it is the elements of this protection mechanism that are mapped to the elements of the TCB.
- Formal analysis techniques must be used to identify and analyze covert channels. Informal techniques may be used to identify covert timing channels. The continued existence of identified covert channels in the system must be justified.

In keeping with the extensive design and development analysis of the TCB required of systems in class (A1), more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

The following are minimal requirements for systems assigned a class (A1) rating:

4.1.1 SECURITY POLICY

4.1.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., access control lists) shall allow users to specify and control sharing of those objects. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

4.1.1.2 Object Reuse

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

4.1.1.3 Labels

Sensitivity labels associated with each ADP system resource (e.g., subject, storage object) that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

4.1.1.3.1 Label Integrity

Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

4.1.1.3.2 Exportation of Labeled Information

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the current security level associated with a single-level communication channel or I/O device.

4.1.1.3.2.1 Exportation to Multilevel Devices

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

4.1.1.3.2.2 Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

4.1.1.3.2.3 Labeling Human-Readable Output

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

4.1.1.3.3 Subject Sensitivity Labels

The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

4.1.1.3.4 Device Labels

The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

4.1.1.4 Mandatory Access Control

The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

---

* The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

4.1.2 ACCOUNTABILITY

4.1.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual user. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

4.1.2.1.1 Trusted Path

The TCB shall support a trusted communication path between itself and users for use when a positive TCB-to-user connection is required (e.g., login, change subject security level). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically isolated and unmistakably distinguishable from other paths.

4.1.2.2 Audit

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels. The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded.

4.1.3 ASSURANCE

4.1.3.1 Operational Assurance

4.1.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.

4.1.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

4.1.3.1.3 Covert Channel Analysis

The system developer shall conduct a thorough search for **covert channels** and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.) **Formal methods shall be used in the analysis.**

4.1.3.1.4 Trusted Facility Management

The TCB shall support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

4.1.3.1.5 Trusted Recovery

Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.

4.1.3.2 Life-Cycle Assurance

4.1.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be found resistant to penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the **formal** top-level specification. (See the Security Testing Guidelines.) No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain. **Manual or other mapping of the FTLS to the source code may form a basis for penetration testing.**

4.1.3.2.2 Design Specification and Verification

A formal model of the security policy supported by the TCB shall be maintained that is proven consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. **A formal top-level specification (FTLS) of the TCB shall be maintained that accurately describes the TCB in terms of exceptions, error messages, and effects. The DTLS and FTLS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface. The FTLS** shall be shown to be an accurate description of the TCB interface. A convincing argument shall be given that the DTLS is consistent with the model **and a combination of formal and informal techniques shall be used to show that the FTLS is consistent with the model. This verification evidence shall be consistent with that provided within the state-of-the-art of the particular Computer Security Center-endorsed formal specification and verification system used. Manual or other mapping of the FTLS to the TCB source code shall be performed to provide evidence of correct implementation.**

4.1.3.2.3 Configuration Management

During **the entire life-cycle, i.e., during the design, development,** and maintenance of the TCB, a configuration management system shall be in place **for all security-relevant hardware, firmware, and software** that maintains control of changes to **the formal model,** the descriptive **and formal** top-level **specifications,** other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools, **maintained under strict configuration control,** for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB. **A combination of technical, physical, and procedural safeguards shall be used to protect from unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.**

4.1.3.2.4 Trusted Distribution

A trusted ADP system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures (e.g., site security acceptance testing) shall exist for assuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies.

4.1.4 DOCUMENTATION

4.1.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

4.1.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described. It shall include the procedures to ensure that the system is initially started in a secure manner. Procedures shall also be included to resume secure system operation after any lapse in system operation.

4.1.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths. **The results of the mapping between the formal top-level specification and the TCB source code shall be given.**

4.1.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of the security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamperproof, cannot be bypassed, and is correctly implemented. The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the **formal top-level specification (FTLS)**. The elements of the **FTLS** shall be shown, using informal techniques, to correspond to the elements of the TCB. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.) **Hardware, firmware, and software mechanisms not dealt with in the FTLS but strictly internal to the TCB (e.g., mapping registers, direct memory access I/O) shall be clearly described.**

4.2 BEYOND CLASS (A1)

Most of the security enhancements envisioned for systems that will provide features and assurance in addition to that already provided by class (A1) systems are beyond current technology. The discussion below is intended to guide future work and is derived from research and development activities already underway in both the public and private sectors. As more and better analysis techniques are developed, the requirements for these systems will become more explicit. In the future, use of formal verification will be extended to the source level and covert timing channels will be more fully addressed. At this level the design environment will become important and testing will be aided by analysis of the formal top-level specification. Consideration will be given to the correctness of the tools used in TCB development (e.g., compilers, assemblers, loaders) and to the correct functioning of the hardware/firmware on which the TCB will run. Areas to be addressed by systems beyond class (A1) include:

* System Architecture

  A demonstration (formal or otherwise) must be given showing that requirements of self-protection and completeness for reference monitors have been implemented in the TCB.

* Security Testing

  Although beyond the current state-of-the-art, it is envisioned that some test-case generation will be done automatically from the formal top-level specification or formal lower-level specifications.

* Formal Specification and Verification

  The TCB must be verified down to the source code level, using formal verification methods where feasible. Formal verification of the source code of the security-relevant portions of an operating system has proven to be a difficult task. Two important considerations are the choice of a high-level language whose semantics can be fully and formally expressed, and a careful mapping, through successive stages, of the abstract formal design to a formalization of the implementation in low-level specifications. Experience has shown that only when the lowest level specifications closely correspond to the actual code can code proofs be successfully accomplished.

* Trusted Design Environment

  The TCB must be designed in a trusted facility with only trusted (cleared) personnel.

PART II:

RATIONALE AND GUIDELINES

5.0 CONTROL OBJECTIVES FOR TRUSTED COMPUTER SYSTEMS

The criteria are divided within each class into groups of requirements. These groupings were developed to assure that three basic control objectives for computer security are satisfied and not overlooked. These control objectives deal with:

- Security Policy
- Accountability
- Assurance

This section provides a discussion of these general control objectives and their implication in terms of designing trusted systems.

5.1 A Need for Consensus

A major goal of the DoD Computer Security Center is to encourage the Computer Industry to develop trusted computer systems and products, making them widely available in the commercial market place. Achievement of this goal will require recognition and articulation by both the public and private sectors of a need and demand for such products.

As described in the introduction to this document, efforts to define the problems and develop solutions associated with processing nationally sensitive information, as well as other sensitive data such as financial, medical, and personnel information used by the National Security Establishment, have been underway for a number of years. The criteria, as described in Part I, represent the culmination of these efforts and describe basic requirements for building trusted computer systems. To date, however, these systems have been viewed by many as only satisfying National Security needs. As long as this perception continues the consensus needed to motivate manufacture of trusted systems will be lacking.

The purpose of this section is to describe, in some detail, the fundamental control objectives that lay the foundations for requirements delineated in the criteria. The goal is to explain the foundations so that those outside the National Security Establishment can assess their universality and, by extension, the universal applicability of the criteria requirements to processing all types of sensitive applications whether they be for National Security or the private sector.

5.2 Definition and Usefulness

The term "control objective" refers to a statement of intent with respect to control over some aspect of an organization's resources, or processes, or both. In terms of a computer system, control objectives provide a framework for developing a strategy for fulfilling a set of security requirements for any given system. Developed in response to generic vulnerabilities, such as the need to manage and handle sensitive data in order to prevent compromise, or the need to provide accountability in order to detect fraud, control objectives have been identified as a useful method of expressing security goals.[3]

Examples of control objectives include the three basic design requirements for implementing the reference monitor concept discussed in Section 6. They are:

- The reference validation mechanism must be tamperproof.

- The reference validation mechanism must always be invoked.
- The reference validation mechanism must be small enough to be subjected to analysis and tests, the completeness of which can be assured.[1]

5.3 Criteria Control Objectives

The three basic control objectives of the criteria are concerned with security policy, accountability, and assurance. The remainder of this section provides a discussion of these basic requirements.

5.3.1 Security Policy

In the most general sense, computer security is concerned with controlling the way in which a computer can be used, i.e., controlling how information processed by it can be accessed and manipulated. However, at closer examination, computer security can refer to a number of areas. Symptomatic of this, FIPS PUB 39, Glossary For Computer Systems Security, does not have a unique definition for computer security.[16] Instead there are eleven separate definitions for security which include: ADP systems security, administrative security, data security, etc. A common thread running through these definitions is the word "protection." Further declarations of protection requirements can be found in DoD Directive 5200.28 which describes an acceptable level of protection for classified data to be one that will "assure that systems which process, store, or use classified data and produce classified information will, with reasonable dependability, prevent: a. Deliberate or inadvertent access to classified material by unauthorized persons, and b. Unauthorized manipulation of the computer and its associated peripheral devices."[8]

In summary, protection requirements must be defined in terms of the perceived threats, risks, and goals of an organization. This is often stated in terms of a security policy. It has been pointed out in the literature that it is external laws, rules, regulations, etc. that establish what access to information is to be permitted, independent of the use of a computer. In particular, a given system can only be said to be secure with respect to its enforcement of some specific policy.[29] Thus, the control objective for security policy is:

SECURITY POLICY CONTROL OBJECTIVE

A STATEMENT OF INTENT WITH REGARD TO CONTROL OVER ACCESS TO AND DISSEMINATION OF INFORMATION, TO BE KNOWN AS THE SECURITY POLICY, MUST BE PRECISELY DEFINED AND IMPLEMENTED FOR EACH SYSTEM THAT IS USED TO PROCESS SENSITIVE INFORMATION. THE SECURITY POLICY MUST ACCURATELY REFLECT THE LAWS, REGULATIONS, AND GENERAL POLICIES FROM WHICH IT IS DERIVED.

5.3.1.1 Mandatory Security Policy

Where a security policy is developed that is to be applied to control of classified or other specifically designated sensitive information, the policy must include detailed rules on how to handle that information throughout its life-cycle. These rules are a function of the various sensitivity designations that the information can assume and the various forms of access supported by the system. Mandatory security refers to the enforcement of a set of access control rules that constrains a subject's access to information on the basis of a comparison of that individual's clearance/authorization to the information, the classification/sensitivity designation of the information, and the form of access being mediated. Mandatory policies either require or can be satisfied by systems that can enforce a partial ordering of designations, namely, the designations must form what is mathematically known as a "lattice."[5]

A clear implication of the above is that the system must assure that the designations associated with sensitive data cannot be arbitrarily changed, since this could permit individuals who lack the appropriate authorization to access sensitive information. Also implied is the requirement that the system control the flow of information so that data cannot be stored with lower sensitivity designations unless its "downgrading" has been authorized. The control objective is:

MANDATORY SECURITY CONTROL OBJECTIVE

SECURITY POLICIES DEFINED FOR SYSTEMS THAT ARE USED TO PROCESS CLASSIFIED OR OTHER SPECIFICALLY CATEGORIZED SENSITIVE INFORMATION MUST INCLUDE PROVISIONS FOR THE ENFORCEMENT OF MANDATORY ACCESS CONTROL RULES. THAT IS, THEY MUST INCLUDE A SET

OF RULES FOR CONTROLLING ACCESS BASED DIRECTLY ON A COMPARISON OF THE INDIVIDUAL'S CLEARANCE OR AUTHORIZATION FOR THE INFORMATION AND THE CLASSIFICATION OR SENSITIVITY DESIGNATION OF THE INFORMATION BEING SOUGHT, AND INDIRECTLY ON CONSIDERATIONS OF PHYSICAL AND OTHER ENVIRONMENTAL FACTORS OF CONTROL. THE MANDATORY ACCESS CONTROL RULES MUST ACCURATELY REFLECT THE LAWS, REGULATIONS, AND GENERAL POLICIES FROM WHICH THEY ARE DERIVED.

5.3.1.2 Discretionary Security Policy

Discretionary security is the principal type of access control available in computer systems today. The basis of this kind of security is that an individual user, or program operating on his behalf, is allowed to specify explicitly the types of access other users may have to information under his control. Discretionary security differs from mandatory security in that it implements an access control policy on the basis of an individual's need-to-know as opposed to mandatory controls which are driven by the classification or sensitivity designation of the information.

Discretionary controls are not a replacement for mandatory controls. In an environment in which information is classified (as in the DoD) discretionary security provides for a finer granularity of control within the overall constraints of the mandatory policy. Access to classified information requires effective implementation of both types of controls as precondition to granting that access. In general, no person may have access to classified information unless: (a) that person has been determined to be trustworthy, i.e., granted a personnel security clearance -- MANDATORY, and (b) access is necessary for the performance of official duties, i.e., determined to have a need-to-know -- DISCRETIONARY. In other words, discretionary controls give individuals discretion to decide on which of the permissible accesses will actually be allowed to which users, consistent with overriding mandatory policy restrictions. The control objective is:

DISCRETIONARY SECURITY CONTROL OBJECTIVE

SECURITY POLICIES DEFINED FOR SYSTEMS THAT ARE USED TO PROCESS CLASSIFIED OR OTHER SENSITIVE

INFORMATION MUST INCLUDE PROVISIONS FOR THE ENFORCEMENT OF DISCRETIONARY ACCESS CONTROL RULES. THAT IS, THEY MUST INCLUDE A CONSISTENT SET OF RULES FOR CONTROLLING AND LIMITING ACCESS BASED ON IDENTIFIED INDIVIDUALS WHO HAVE BEEN DETERMINED TO HAVE A NEED-TO-KNOW FOR THE INFORMATION.

5.3.1.3 Marking

To implement a set of mechanisms that will put into effect a mandatory security policy, it is necessary that the system mark information with appropriate classification or sensitivity labels and maintain these markings as the information moves through the system. Once information is unalterably and accurately marked, comparisons required by the mandatory access control rules can be accurately and consistently made. An additional benefit of having the system maintain the classification or sensitivity label internally is the ability to automatically generate properly "labeled" output. The labels, if accurately and integrally maintained by the system, remain accurate when output from the system. The control objective is:

MARKING CONTROL OBJECTIVE

SYSTEMS THAT ARE DESIGNED TO ENFORCE A MANDATORY SECURITY POLICY MUST STORE AND PRESERVE THE INTEGRITY OF CLASSIFICATION OR OTHER SENSITIVITY LABELS FOR ALL INFORMATION. LABELS EXPORTED FROM THE SYSTEM MUST BE ACCURATE REPRESENTATIONS OF THE CORRESPONDING INTERNAL SENSITIVITY LABELS BEING EXPORTED.

5.3.2 Accountability

The second basic control objective addresses one of the fundamental principles of security, i.e., individual accountability. Individual accountability is the key to securing and controlling any system that processes information on behalf of individuals or groups of individuals. A number of requirements must be met in order to satisfy this objective.

The first requirement is for individual user identification. Second, there is a need for authentication of the identification. Identification is functionally dependent on authentication. Without authentication, user identification has no credibility. Without a credible identity, neither mandatory nor discretionary security policies can be properly invoked because there is no assurance that proper authorizations can be made.

The third requirement is for dependable audit capabilities. That is, a trusted computer system must provide authorized personnel with the ability to audit any action that can potentially cause access to, generation of, or effect the release of classified or sensitive information. The audit data will be selectively acquired based on the auditing needs of a particular installation and/or application. However, there must be sufficient granularity in the audit data to support tracing the auditable events to a specific individual who has taken the actions or on whose behalf the actions were taken. The control objective is:

ACCOUNTABILITY CONTROL OBJECTIVE

SYSTEMS THAT ARE USED TO PROCESS OR HANDLE CLASSIFIED OR OTHER SENSITIVE INFORMATION MUST ASSURE INDIVIDUAL ACCOUNTABILITY WHENEVER EITHER A MANDATORY OR DISCRETIONARY SECURITY POLICY IS INVOKED. FURTHERMORE, TO ASSURE ACCOUNTABILITY THE CAPABILITY MUST EXIST FOR AN AUTHORIZED AND COMPETENT AGENT TO ACCESS AND EVALUATE ACCOUNTABILITY INFORMATION BY A SECURE MEANS, WITHIN A REASONABLE AMOUNT OF TIME, AND WITHOUT UNDUE DIFFICULTY.

5.3.3 Assurance

The third basic control objective is concerned with guaranteeing or providing confidence that the security policy has been implemented correctly and that the protection-relevant elements of the system do, indeed, accurately mediate and enforce the intent of that policy. By extension, assurance must include a guarantee that the trusted portion of the system works only as intended. To accomplish these objectives, two types of assurance are needed. They are life-cycle assurance and operational assurance.

Life-cycle assurance refers to steps taken by an organization to ensure that the system is designed, developed, and maintained using formalized and rigorous controls and standards.[17] Computer systems that process and store sensitive or classified information depend on the hardware and software to protect that information. It follows that the hardware and software themselves must be protected against unauthorized changes that could cause protection mechanisms to malfunction or be bypassed completely. For this reason trusted computer systems must be carefully evaluated and tested during the design and development phases and reevaluated whenever changes are made that could affect the integrity of the protection mechanisms. Only in this way can confidence be provided that the hardware and software interpretation of the security policy is maintained accurately and without distortion.

While life-cycle assurance is concerned with procedures for managing system design, development, and maintenance; operational assurance focuses on features and system architecture used to ensure that the security policy is uncircumventably enforced during system operation. That is, the security policy must be integrated into the hardware and software protection features of the system. Examples of steps taken to provide this kind of confidence include: methods for testing the operational hardware and software for correct operation, isolation of protection-critical code, and the use of hardware and software to provide distinct domains. The control objective is:

ASSURANCE CONTROL OBJECTIVE

SYSTEMS THAT ARE USED TO PROCESS OR HANDLE CLASSIFIED OR OTHER SENSITIVE INFORMATION MUST BE DESIGNED TO GUARANTEE CORRECT AND ACCURATE INTERPRETATION OF THE SECURITY POLICY AND MUST NOT DISTORT THE INTENT OF THAT POLICY. ASSURANCE MUST BE PROVIDED THAT CORRECT IMPLEMENTATION AND OPERATION OF THE POLICY EXISTS THROUGHOUT THE SYSTEM'S LIFE-CYCLE.

6.0 RATIONALE BEHIND THE EVALUATION CLASSES

6.1 The Reference Monitor Concept

In October of 1972, the Computer Security Technology Planning Study, conducted by James P. Anderson & Co., produced a report for the Electronic Systems Division (ESD) of the United States Air Force.[1] In that report, the concept of "a reference monitor which enforces the authorized access relationships between subjects and objects of a system" was introduced. The reference monitor concept was found to be an essential element of any system that would provide multilevel secure computing facilities and controls.

The Anderson report went on to define the reference validation mechanism as "an implementation of the reference monitor concept . . . that validates each reference to data or programs by any user (program) against a list of authorized types of reference for that user." It then listed the three design requirements that must be met by a reference validation mechanism:

> "a. The reference validation mechanism must be tamper proof.
>
> b. The reference validation mechanism must always be invoked.
>
> c. The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured."[1]

Extensive peer review and continuing research and development activities have sustained the validity of the Anderson Committee's findings. Early examples of the reference validation mechanism were known as security kernels. The Anderson Report described the security kernel as "that combination of hardware and software which implements the reference monitor concept."[1] In this vein, it will be noted that the security kernel must support the three reference monitor requirements listed above.

6.2 A Formal Security Policy Model

Following the publication of the Anderson report, considerable research was initiated into formal models of security policy requirements and of the mechanisms that would implement and enforce those policy models as a security kernel. Prominent among these efforts was the ESD-sponsored development of the Bell and LaPadula model, an abstract formal treatment of DoD security policy.[2] Using mathematics and set theory, the model precisely defines the notion of secure state, fundamental modes of access, and the rules for granting subjects specific modes of access to objects. Finally, a theorem is proven to demonstrate that the rules are security-preserving operations, so that the application of any sequence of the rules to a system that is in a secure state will result in the system entering a new state that is also secure. This theorem is known as the Basic Security Theorem.

The Bell and LaPadula model defines a relationship between clearances of subjects and classifications of system objects, now referenced as the "dominance relation." From this definition, accesses permitted between subjects and objects are explicitly defined for the fundamental modes of access, including read-only access, read/write access, and write-only access. The model defines the Simple Security Condition to control granting a subject read access to a specific object, and the *-Property (read "Star Property") to control granting a subject write access to a specific object. Both the Simple Security Condition and the *-Property include mandatory security provisions based on the dominance relation between the clearance of the subject and the classification of the object. The Discretionary Security Property is also defined, and requires that a specific subject be authorized for the particular mode of access required for the state transition. In its treatment of subjects (processes acting on behalf of a user), the model distinguishes between trusted subjects (i.e., not constrained within the model by the *-Property) and untrusted subjects (those that are constrained by the *-Property).

From the Bell and LaPadula model there evolved a model of the method of proof required to formally demonstrate that all arbitrary sequences of state transitions are security-preserving. It was also shown that the *-Property is sufficient to prevent the compromise of information by Trojan Horse attacks.

6.3 The Trusted Computing Base

In order to encourage the widespread commercial availability of trusted computer systems, these evaluation criteria have been designed to address those systems in which a security kernel is specifically implemented as well as those in which a security kernel has not been implemented. The latter case includes those systems in which objective (c) is not fully supported because of the size or complexity of the reference validation mechanism. For convenience, these evaluation criteria use the term Trusted Computing Base to refer to the reference validation mechanism, be it a security kernel, front-end security filter, or the entire trusted computer system.

The heart of a trusted computer system is the Trusted Computing Base (TCB) which contains all of the elements of the system responsible for supporting the security policy and supporting the isolation of objects (code and data) on which the protection is based. The bounds of the TCB equate to the "security perimeter" referenced in some computer security literature. In the interest of understandable and maintainable protection, a TCB should be as simple as possible consistent with the functions it has to perform. Thus, the TCB includes hardware, firmware, and software critical to protection and must be designed and implemented such that system elements excluded from it need not be trusted to maintain protection. Identification of the interface and elements of the TCB along with their correct functionality therefore forms the basis for evaluation.

For general-purpose systems, the TCB will include key elements of the operating system and may include all of the operating system. For embedded systems, the security policy may deal with objects in a way that is meaningful at the application level rather than at the operating system level. Thus, the protection policy may be enforced in the application software rather than in the underlying operating system. The TCB will necessarily include all those portions of the operating system and application software essential to the support of the policy. Note that, as the amount of code in the TCB increases, it becomes harder to be confident that the TCB enforces the reference monitor requirements under all circumstances.

6.4 Assurance

The third reference monitor design objective is currently interpreted as meaning that the TCB "must be of sufficiently simple organization and complexity to be subjected to analysis and tests, the completeness of which can be assured."

Clearly, as the perceived degree of risk increases (e.g., the range of sensitivity of the system's protected data, along with the range of clearances held by the system's user population) for a particular system's operational application and environment, so also must the assurances be increased to substantiate the degree of trust that will be placed in the system. The hierarchy of requirements that are presented for the evaluation classes in the trusted computer system evaluation criteria reflect the need for these assurances.

As discussed in Section 5.3, the evaluation criteria uniformly require a statement of the security policy that is enforced by each trusted computer system. In addition, it is required that a convincing argument be presented that explains why the TCB satisfies the first two design requirements for a reference monitor. It is not expected that this argument will be entirely formal. This argument is required for each candidate system in order to satisfy the assurance control objective.

The systems to which security enforcement mechanisms have been added, rather than built-in as fundamental design objectives, are not readily amenable to extensive analysis since they lack the requisite conceptual simplicity of a security kernel. This is because their TCB extends to cover much of the entire system. Hence, their degree of trustworthiness can best be ascertained only by obtaining test results. Since no test procedure for something as complex as a computer system can be truly exhaustive, there is always the possibility that a subsequent penetration attempt could succeed. It is for this reason that such systems must fall into the lower evaluation classes.

On the other hand, those systems that are designed and engineered to support the TCB concepts are more amenable to analysis and structured testing. Formal methods can be used to analyze the correctness of their reference validation mechanisms in enforcing the system's security policy. Other methods, including less-formal arguments, can be used in order to substantiate claims for the completeness of their access mediation and their degree of tamper-resistance. More confidence can be placed in the results of this analysis and in the thoroughness of the structured testing than can be placed in the results for less methodically structured systems. For these reasons, it appears reasonable to conclude that these systems could be used in higher-risk environments. Successful implementations of such systems would be placed in the higher evaluation classes.

6.5 The Classes

It is highly desirable that there be only a small number of overall evaluation classes. Three major divisions have been identified in the evaluation criteria with a fourth division reserved for those systems that have been evaluated and found to offer unacceptable security protection. Within each major evaluation division, it was found that "intermediate" classes of trusted system design and development could meaningfully be defined. These intermediate classes have been designated in the criteria because they identify systems that:

* are viewed to offer significantly better protection and assurance than would systems that satisfy the basic requirements for their evaluation class; and

* there is reason to believe that systems in the intermediate evaluation classes could eventually be evolved such that they would satisfy the requirements for the next higher evaluation class.

Except within division A it is not anticipated that additional "intermediate" evaluation classes satisfying the two characteristics described above will be identified.

Distinctions in terms of system architecture, security policy enforcement, and evidence of credibility between evaluation classes have been defined such that the "jump" between evaluation classes would require a considerable investment of effort on the part of implementors. Correspondingly, there are expected to be significant differentials of risk to which systems from the higher evaluation classes will be exposed.

7.0 THE RELATIONSHIP BETWEEN POLICY AND THE CRITERIA

Section 1 presents fundamental computer security requirements and Section 5 presents the control objectives for Trusted Computer Systems. They are general requirements, useful and necessary, for the development of all secure systems. However, when designing systems that will be used to process classified or other sensitive information, functional requirements for meeting the Control Objectives become more specific. There is a large body of policy laid down in the form of Regulations, Directives, Presidential Executive Orders, and OMB Circulars that form the basis of the procedures for the handling and processing of Federal information in general and classified information specifically. This section presents pertinent excerpts from these policy statements and discusses their relationship to the Control Objectives.

7.1 Established Federal Policies

A significant number of computer security policies and associated requirements have been promulgated by Federal government elements. The interested reader is referred to reference [31] which analyzes the need for trusted systems in the civilian agencies of the Federal government, as well as in state and local governments and in the private sector. This reference also details a number of relevant Federal statutes, policies and requirements not treated further below.

Security guidance for Federal automated information systems is provided by the Office of Management and Budget. Two specifically applicable Circulars have been issued. OMB Circular No. A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems,"[25] directs each executive agency to establish and maintain a computer security program. It makes the head of each executive branch, department and agency responsible "for assuring an adequate level of security for all agency data whether processed in-house or commercially. This includes responsibility for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data not subject to national security regulations, as well as national security data."[25, para. 4 p. 2]

OMB Circular No. A-123, "Internal Control Systems,"[26] issued to help eliminate fraud, waste, and abuse in government programs requires: (a) agency heads to issue internal control directives and assign responsibility, (b) managers to review programs for vulnerability, and (c) managers to perform periodic reviews to evaluate strengths and update controls. Soon after promulgation of OMB Circular A-123, the relationship of its internal control requirements to building secure computer systems was recognized.[4] While not stipulating computer controls specifically, the definition of Internal Controls in A-123 makes it clear that computer systems are to be included:

> "Internal Controls - The plan of organization and all of the methods and measures adopted within an agency to safeguard its resources, assure the accuracy and reliability of its information, assure adherence to applicable laws, regulations and policies, and promote operational economy and efficiency."[26, sec. 4.C]

The matter of classified national security information processed by ADP systems was one of the first areas given serious and extensive concern in computer security. The computer security policy documents promulgated as a result contain generally more specific and structured requirements than most, keyed in turn to an authoritative basis that itself provides a rather clearly articulated and structured information security policy. This basis, Executive Order 12356, "National Security Information," sets forth requirements for the classification, declassification and safeguarding of "national security information" per se.[14]

7.2 DoD Policies

Within the Department of Defense, these broad requirements are implemented and further specified primarily through two vehicles: 1) DoD Regulation 5200.1-R [7], which applies to all components of the DoD as such, and 2) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information" [11], which applies to contractors included within the Defense Industrial Security Program. Note that the latter transcends DoD as such, since it applies not only to any contractors handling classified information for any DoD component, but also to the contractors of eighteen other Federal organizations for whom the Secretary of Defense is authorized to act in rendering industrial security services.*

For ADP systems, these information security requirements are further amplified and specified in: 1) DoD Directive 5200.28 [8] and DoD Manual 5200.28-M [9], for DoD components; and 2) Section XIII of DoD 5220.22-M [11] for contractors. DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," stipulates: "Classified material contained in an ADP system shall be safeguarded by the continuous employment of protective features in the system's hardware and software design and configuration . . . ."[8, sec. IV] Furthermore, it is required that ADP systems that "process, store, or use classified data and produce classified information will, with reasonable dependability, prevent:

a. Deliberate or inadvertent access to classified material by unauthorized persons, and

---

* i.e., NASA, Commerce Department, GSA, State Department, Small Business Administration, National Science Foundation, Treasury Department, Transportation Department, Interior Department, Agriculture Department, Health and Human Services Department, Labor Department, Environmental Protection Agency, Justice Department, U.S. Arms Control and Disarmament Agency, Federal Emergency Management Agency, Federal Reserve System, and U.S. General Accounting Office.

b. Unauthorized manipulation of the computer and its associated peripheral devices."[8, sec. I B.3]

Requirements equivalent to these appear within DoD 5200.28-M [9] and in DoD 5220.22-M [11].

From requirements imposed by these regulations, directives and circulars, the three components of the Security Policy Control Objective, i.e., Mandatory and Discretionary Security and Marking, as well as the Accountability and Assurance Control Objectives, can be functionally defined for DoD applications. The following discussion provides further specificity in Policy for these Control Objectives.

7.3 Criteria Control Objective for Security Policy

7.3.1 Marking

The control objective for marking is: "Systems that are designed to enforce a mandatory security policy must store and preserve the integrity of classification or other sensitivity labels for all information. Labels exported from the system must be accurate representations of the corresonding internal sensitivity labels being exported."

DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," explains in paragraph 11 the reasons for marking information:

"Designation by physical marking, notation or other means serves to inform and to warn the holder about the classification designation of the information which requires protection in the interest of national security. The degree of protection against unauthorized disclosure which will be required for a particular level of classification is directly commensurate with the marking designation which is assigned to the material."[11]

Marking requirements are given in a number of policy statements.

Executive Order 12356 (Sections 1.5.a and 1.5.a.1) requires that classification markings "shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved."[14]

DoD Regulation 5200.1-R (Section 1-500) requires that: ". . . information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations, namely: 'Top Secret,' 'Secret' or 'Confidential.'"[7] (By extension, for use in computer processing, the unofficial designation "Unclassified" is used to indicate information that does not fall under one of the other three designations of classified information.)

DoD Regulation 5200.1-R (Section 4-304b) requires that: "ADP systems and word processing systems employing such media shall provide for internal classification marking to assure that classified information contained therein that is reproduced or generated, will bear applicable classification and associated markings." (This regulation provides for the exemption of certain existing systems where "internal classification and applicable associated markings cannot be implemented without extensive system modifications."[7] However, it is clear that future DoD ADP systems must be able to provide applicable and accurate labels for classified and other sensitive information.)

DoD Manual 5200.28-M (Section IV, 4-305d) requires the following: "Security Labels - All classified material accessible by or within the ADP system shall be identified as to its security classification and access or dissemination limitations, and all output of the ADP system shall be appropriately marked."[9]

7.3.2 Mandatory Security

The control objective for mandatory security is: "Security policies defined for systems that are used to process classified or other specifically categorized sensitive information must include provisions for the enforcement of mandatory access control rules. That is, they must include a set of rules for controlling access based directly on a comparison of the individual's clearance or authorization for the information and the classification or sensitivity designation of the information being sought, and indirectly on considerations of physical and other environmental factors of control. The mandatory access control rules must accurately reflect the laws, regulations, and general policies from which they are derived."

There are a number of policy statements that are related to mandatory security.

Executive Order 12356 (Section 4.1.a) states that "a person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes."[14]

DoD Regulation 5200.1-R (Chapter I, Section 3) defines a Special Access Program as "any program imposing 'need-to-know' or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements, special designation of officials authorized to determine 'need-to-know', or special lists of persons determined to have a 'need-to-know.'"[7, para. 1-328] This passage distinguishes between a 'discretionary' determination of need-to-know and formal need-to-know which is implemented through Special Access Programs. DoD Regulation 5200.1-R, paragraph 7-100 describes general requirements for trustworthiness (clearance) and need-to-know, and states that the individual with possession, knowledge or control of classified information has final responsibility for determining if conditions for access have been met. This regulation further stipulates that "no one has a right to have access to classified information solely by virtue of rank or position." [7, para. 7-100])

DoD Manual 5200.28-M (Section II 2-100) states that, "Personnel who develop, test (debug), maintain, or use programs which are classified or which will be used to access or develop classified material shall have a personnel security clearance and an access authorization (need-to-know), as appropriate for the highest classified and most restrictive category of classified material which they will access under system constraints."[9]

DoD Manual 5220.22-M (Paragraph 3.a) defines access as "the ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures which are in force do not prevent him from gaining knowledge of the classified information."[11]

The above mentioned Executive Order, Manual, Directives and Regulations clearly imply that a trusted computer system must assure that the classification labels associated with sensitive data cannot be arbitrarily changed, since this could permit individuals who lack the appropriate clearance to access classified information. Also implied is the requirement that a trusted computer system must control the flow of information so that data from a higher classification cannot be placed in a storage object of lower classification unless its "downgrading" has been authorized.

7.3.3 Discretionary Security

The term discretionary security refers to a computer system's ability to control information on an individual basis. It stems from the fact that even though an individual has all the formal clearances for access to specific classified information, each individual's access to information must be based on a demonstrated need-to-know. Because of this, it must be made clear that this requirement is not discretionary in a "take it or leave it" sense. The directives and regulations are explicit in stating that the need-to-know test must be satisfied before access can be granted to the classified information. The control objective for discretionary security is: "Security policies defined for systems that are used to process classified or other sensitive information must include provisions for the enforcement of discretionary access control rules. That is, they must include a consistent set of rules for controlling and limiting access based on identified individuals who have been determined to have a need-to-know for the information."

DoD Regulation 5200.1-R (Paragraph 7-100) In addition to excerpts already provided that touch on need-to-know, this section of the regulation stresses the need-to-know principle when it states "no person may have access to classified information unless . . . access is necessary for the performance of official duties."[7]

Also, **DoD Manual 5220.22-M** (Section III 20.a) states that "an individual shall be permitted to have access to classified information only . . . when the contractor determines that access is necessary in the performance of tasks or services essential to the fulfillment of a contract or program, i.e., the individual has a need-to-know."[11]

7.4 Criteria Control Objective for Accountability

The control objective for accountability is: "Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time, and without undue difficulty."

This control objective is supported by the following citations:

DoD Directive 5200.28 (VI.A.1) states: "Each user's identity shall be positively established, and his access to the system, and his activity in the system (including material accessed and actions taken) controlled and open to scrutiny."[8]

DoD Manual 5200.28-M (Section V 5-100) states: "An audit log or file (manual, machine, or a combination of both) shall be maintained as a history of the use of the ADP System to permit a regular security review of system activity. (e.g., The log should record security related transactions, including each access to a classified file and the nature of the access, e.g., logins, production of accountable classified outputs, and creation of new classified files. Each classified file successfully accessed [regardless of the number of individual references] during each 'job' or 'interactive session' should also be recorded in the audit log. Much of the material in this log may also be required to assure that the system preserves information entrusted to it.)"[9]

DoD Manual 5200.28-M (Section IV 4-305f) states: "Where needed to assure control of access and individual accountability, each user or specific group of users shall be identified to the ADP System by appropriate administrative or hardware/software measures. Such identification measures must be in sufficient detail to enable the ADP System to provide the user only that material which he is authorized."[9]

DoD Manual 5200.28-M (Section I 1-102b) states: "Component's Designated Approving Authorities, or their designees for this purpose . . . will assure:

. . . .

(4) Maintenance of documentation on operating systems (O/S) and all modifications thereto, and its retention for a sufficient period of time to enable tracing of security-related defects to their point of origin or inclusion in the system.

. . . .

(6) Establishment of procedures to discover, recover, handle, and dispose of classified material improperly disclosed through system malfunction or personnel action.

(7) Proper disposition and correction of security deficiencies in all approved ADP Systems, and the effective use and disposition of system housekeeping or audit records, records of security violations or security-related system malfunctions, and records of tests of the security features of an ADP System."[9]

DoD Manual 5220.22-M (Section XIII 111) states: "Audit Trails

a. The general security requirement for any ADP system audit trail is that it provide a documented history of the use of the system. An approved audit trail will permit review of classified system activity and will provide a detailed activity record to facilitate reconstruction of events to determine the magnitude of compromise (if any) should a security malfunction occur. To fulfill this basic requirement, audit trail systems, manual, automated or a combination of both must document significant events occurring in the following areas of concern: (i) preparation of input data and dissemination of output data (i.e., reportable interactivity between users and system support personnel), (ii) activity involved within an ADP environment (e.g., ADP support personnel modification of security and related controls), and (iii) internal machine activity.

b. The audit trail for an ADP system approved to process classified information must be based on the above three areas and may be stylized to the particular system. All systems approved for classified processing should contain most if not all of the audit trail records listed below. The contractor's SPP documentation must identify and describe those applicable:

1. Personnel access;

2. Unauthorized and surreptitious entry into the central computer facility or remote terminal areas;

3. Start/stop time of classified processing indicating pertinent systems security initiation and termination events (e.g., upgrading/downgrading actions pursuant to paragraph 107);

4. All functions initiated by ADP system console operators;

5. Disconnects of remote terminals and peripheral devices (paragraph 107c);

6. Log-on and log-off user activity;

7. Unauthorized attempts to access files or programs, as well as all open, close, create, and file destroy actions;

8. Program aborts and anomalies including identification information (i.e., user/program name, time and location of incident, etc.);

9. System hardware additions, deletions and maintenance actions;

10. Generations and modifications affecting the security features of the system software.

c. The ADP system security supervisor or designee shall review the audit trail logs at least weekly to assure that all pertinent activity is properly recorded and that appropriate action has been taken to correct any anomaly. The majority of ADP systems in use today can develop audit trail systems in accord with the above; however, special systems such as weapons, communications, communications security, and tactical data exchange and display systems, may not be able to comply with all aspects of the above and may require individualized consideration by the cognizant security office.

d. Audit trail records shall be retained for a period of one inspection cycle."[11]

7.5 Criteria Control Objective for Assurance

The control objective for assurance is: "Systems that are used to process or handle classified or other sensitive information must be designed to guarantee correct and accurate interpretation of the security policy and must not distort the intent of that policy. Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life-cycle."

A basis for this objective can be found in the following sections of DoD Directive 5200.28:

DoD Directive 5200.28 (IV.B.1) stipulates: "Generally, security of an ADP system is most effective and economical if the system is designed originally to provide it. Each Department of Defense Component undertaking design of an ADP system which is expected to process, store, use, or produce classified material shall: From the beginning of the design process, consider the security policies, concepts, and measures prescribed in this Directive."[8]

DoD Directive 5200.28 (IV.C.5.a) states: "Provision may be made to permit adjustment of ADP system area controls to the level of protection required for the classification category and type(s) of material actually being handled by the system, provided change procedures are developed and implemented which will prevent both the unauthorized access to classified material handled by the system and the unauthorized manipulation of the system and its components. Particular attention shall be given to the continuous protection of automated system security measures, techniques and procedures when the personnel security clearance level of users having access to the system changes."[8]

DoD Directive 5200.28 (VI.A.2) states: "Environmental Control. The ADP System shall be externally protected to minimize the likelihood of unauthorized access to system entry points, access to classified information in the system, or damage to the system."[8]

DoD Manual 5200.28-M (Section I 1-102b) states: "Component's Designated Approving Authorities, or their designees for this purpose . . . will assure:

. . . .

(5) Supervision, monitoring, and testing, as appropriate, of changes in an approved ADP System which could affect the security features of the system, so that a secure system is maintained.

. . . .

(7) Proper disposition and correction of security deficiencies in all approved ADP Systems, and the effective use and disposition of system housekeeping or audit records, records of security violations or security-related system malfunctions, and records of tests of the security features of an ADP System.

(8) Conduct of competent system ST&E, timely review of system ST&E reports, and correction of deficiencies needed to support conditional or final approval or disapproval of an ADP System for the processing of classified information.

(9) Establishment, where appropriate, of a central ST&E coordination point for the maintenance of records of selected techniques, procedures, standards, and tests used in the testing and evaluation of security features of ADP

Systems which may be suitable for validation and use by other Department of Defense Components."[9]

DoD Manual 5220.22-M (Section XIII 103a) requires: "the initial approval, in writing, of the cognizant security office prior to processing any classified information in an ADP system. This section requires reapproval by the cognizant security office for major system modifications made subsequent to initial approval. Reapprovals will be required because of (i) major changes in personnel access requirements, (ii) relocation or structural modification of the central computer facility, (iii) additions, deletions or changes to main frame, storage or input/output devices, (iv) system software changes impacting security protection features, (v) any change in clearance, declassification, audit trail or hardware/software maintenance procedures, and (vi) other system changes as determined by the cognizant security office."[11]

A major component of assurance, life-cycle assurance, is concerned with testing ADP systems both in the development phase as well as during operation. **DoD Directive 5215.1** (Section F.2.C.(2)) requires "evaluations of selected industry and government-developed trusted computer systems against these criteria."[10]

8.0 A GUIDELINE ON COVERT CHANNELS

A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy. There are two types of covert channels: storage channels and timing channels. Covert storage channels include all vehicles that would allow the direct or indirect writing of a storage location by one process and the direct or indirect reading of it by another. Covert timing channels include all vehicles, that would allow one process to signal information to another process by modulating its own use of system resources in such a way that the change in response time observed by the second process would provide information.

From a security perspective, covert channels with low bandwidths represent a lower threat than those with high bandwidths. However, for many types of covert channels, techniques used to reduce the bandwidth below a certain rate (which depends on the specific channel mechanism and the system architecture) also have the effect of degrading the performance provided to legitimate system users. Hence, a trade-off between system performance and covert channel bandwidth must be made. Because of the threat of compromise that would be present in any multilevel computer system containing classified or sensitive information, such systems should not contain covert channels with high bandwidths. This guideline is intended to provide system developers with an idea of just how high a "high" covert channel bandwidth is.

A covert channel bandwidth that exceeds a rate of one hundred (100) bits per second is considered "high" because 100 bits per second is the approximate rate at which many computer terminals are run. It does not seem appropriate to call a computer system "secure" if information can be compromised at a rate equal to the normal output rate of some commonly used device.

In any multilevel computer system there are a number of relatively low-bandwidth covert channels whose existence is deeply ingrained in the system design. Faced with the large potential cost of reducing the bandwidths of such covert channels, it is felt that those with maximum bandwidths of less than one (1) bit per second are acceptable in most application environments. Though maintaining acceptable performance in some systems may make it impractical to eliminate all covert channels with bandwidths of 1 or more bits per second, it is possible to audit their use without adversely affecting system performance. This audit capability provides the system administration with a means of detecting -- and procedurally correcting -- significant compromise. Therefore, a Trusted Computing Base should provide, wherever possible, the capability to audit the use of covert channel mechanisms with bandwidths that may exceed a rate of one (1) bit in ten (10) seconds.

The covert channel problem has been addressed by a number of authors. The interested reader is referred to references [5], [6], [18], [20], [21], [22], and [28].

9.0 A GUIDELINE ON CONFIGURING MANDATORY ACCESS CONTROL FEATURES

The Mandatory Access Control requirement includes a capability to support an unspecified number of hierarchical classifications and an unspecified number of non-hierarchical categories at each hierarchical level. To encourage consistency and portability in the design and development of the National Security Establishment trusted computer systems, it is desirable for all such systems to be able to support a minimum number of levels and categories. The following suggestions are provided for this purpose:

- The number of hierarchical classifications should be greater than or equal to eight (8).
- The number of non-hierarchical categories should be greater than or equal to twenty-nine (29).

10.0 A GUIDELINE ON SECURITY TESTING

These guidelines are provided to give an indication of the extent and sophistication of testing undertaken by the DoD Computer Security Center during the Formal Product Evaluation process. Organizations wishing to use "Department of Defense Trusted Computer System Evaluation Criteria" for performing their own evaluations may find this section useful for planning purposes.

As in Part I, highlighting is used to indicate changes in the guidelines from the next lower division.

10.1 Testing for Division C

10.1.1 Personnel

The security testing team shall consist of at least two individuals with bachelor degrees in Computer Science or the equivalent. Team members shall be able to follow test plans prepared by the system developer and suggest additions, shall be familiar with the "flaw hypothesis" or equivalent security testing methodology, and shall have assembly level programming experience. Before testing begins, the team members shall have functional knowledge of, and shall have completed the system developer's internals course for, the system being evaluated.

10.1.2 Testing

The team shall have "hands-on" involvement in an independent run of the tests used by the system developer. The team shall independently design and implement at least five system-specific tests in an attempt to circumvent the security mechanisms of the system. The elapsed time devoted to testing shall be at least one month and need not exceed three months. There shall be no fewer than twenty hands-on hours spent carrying out system developer-defined tests and test team-defined tests.

10.2 Testing for Division B

10.2.1 Personnel

The security testing team shall consist of at least two individuals with bachelor degrees in Computer Science or the equivalent **and at least one individual with a master's degree in Computer Science or equivalent.** Team members shall be able to follow test plans prepared by the system developer and suggest additions, shall be **conversant** with the "flaw hypothesis" or equivalent security testing methodology, **shall be fluent in the TCB implementation language(s)**, and shall have assembly level programming experience. Before testing begins, the team members shall have functional knowledge of, and shall have completed the system developer's internals course for, the system being evaluated. **At least one team member shall have previously completed a security test on another system.**

10.2.2 Testing

The team shall have "hands-on" involvement in an independent run of the **test package** used by the system developer **to test security-relevant hardware and software**. The team shall independently design and implement at least **fifteen** system-specific tests in an attempt to circumvent the security mechanisms of the system. The elapsed time devoted to testing shall be at least **two months** and need not exceed **four** months. There shall be no fewer than **thirty** hands-on hours **per team member** spent carrying out system developer-defined tests and test team-defined tests.

10.3 Testing for Division A

10.3.1 Personnel

The security testing team shall consist of at least **one individual with a bachelor's degree** in Computer Science or the equivalent and at least **two individuals** with **masters' degrees** in Computer Science or equivalent. Team members shall be able to follow test plans prepared by the system developer and suggest additions, shall be conversant with the "flaw hypothesis" or equivalent security testing methodology, shall be fluent in the TCB implementation language(s), and shall have assembly level programming experience. Before testing begins, the team members shall have functional knowledge of, and shall have completed the system developer's internals course for, the system being evaluated. **At least one team member shall be familiar enough with the system hardware to understand the maintenance diagnostic programs and supporting hardware documentation.** At least **two** team **members** shall have previously completed a security test on another system. **At least one team member shall have demonstrated system level programming competence on the system under test to a level of complexity equivalent to adding a device driver to the system.**

10.3.2 Testing

The team shall have "hands-on" involvement in an independent run of the test package used by the system developer to test security-relevant hardware and software. The team shall independently design and implement at least **twenty-five** system-specific tests in an attempt to circumvent the security mechanisms of the system. The elapsed time devoted to testing shall be at least **three** months and need not exceed **six** months. There shall be no fewer than **fifty** hands-on hours per team member spent carrying out system developer-defined tests and test team-defined tests.

APPENDIX A

Commercial Product Evaluation Process

"Department of Defense Trusted Computer System Evaluation Criteria" forms the basis upon which the Computer Security Center will carry out the commercial computer security evaluation process. This process is focused on commercially produced and supported general-purpose operating system products that meet the needs of government departments and agencies. The formal evaluation is aimed at "off-the-shelf" commercially supported products and is completely divorced from any consideration of overall system performance, potential applications, or particular processing environments. The evaluation provides a key input to a computer system security approval/accreditation. However, it does not constitute a complete computer system security evaluation. A complete study must consider additional factors dealing with the system in its unique environment, such as it's proposed security mode of operation, specific users, applications, data sensitivity, physical and personnel security, administrative and procedural security, TEMPEST, and communications security.

The product evaluation process carried out by the Computer Security Center has three distinct elements:

* Preliminary Product Evaluation - An informal dialogue between a vendor and the Center in which technical information is exchanged to create a common understanding of the vendor's product, the criteria, and the rating that may be expected to result from a formal product evaluation.

* Formal Product Evaluation - A formal evaluation, by the Center, of a product that is available to the DoD, and that results in that product and its assigned rating being placed on the Evaluated Products List.

* Evaluated Products List - A list of products that have been subjected to formal product evaluation and their assigned ratings.

Preliminary Product Evaluation

Since it is generally very difficult to add effective security measures late in a product's life cycle, the Center is interested in working with system vendors in the early stages of product design. A preliminary product evaluation allows the Center to consult with computer vendors on computer security issues found in products that have not yet been formally announced.

A preliminary evaluation is typically initiated by computer system vendors who are planning new computer products that feature security or major security-related upgrades to existing products. After an initial meeting between the vendor and the Center, appropriate non-disclosure agreements are executed that require the Center to maintain the confidentiality of any proprietary information disclosed to it. Technical exchange meetings follow in which the vendor provides details about the proposed product (particularly its internal designs and goals) and the Center provides expert feedback to the vendor on potential computer security strengths and weaknesses of the vendor's design choices, as well as relevant interpretation of the criteria. The preliminary evaluation is typically terminated when the product is completed and ready for field release by the vendor. Upon termination, the Center prepares a wrap-up report for the vendor and for internal distribution within the Center. Those reports containing proprietary information are not available to the public.

During preliminary evaluation, the vendor is under no obligation to actually complete or market the potential product. The Center is, likewise, not committed to conduct a formal product evaluation. A preliminary evaluation may be terminated by either the Center or the vendor when one notifies the other, in writing, that it is no longer advantageous to continue the evaluation.

Formal Product Evaluation

The formal product evaluation provides a key input to certification of a computer system for use in National Security Establishment applications and is the sole basis for a product being placed on the Evaluated Products List.

A formal product evaluation begins with a request by a vendor for the Center to evaluate a product for which the product itself and accompanying documentation needed to meet the requirements defined by this publication are complete. Non-disclosure agreements are executed and a formal product evaluation team is formed by the Center. An initial meeting is then held with the vendor to work out the schedule for the formal evaluation. Since testing of the implemented product forms an important part of the evaluation process, access by the evaluation team to a working version of the system is negotiated with the vendor. Additional support required from the vendor includes complete design documentation, source code, and access to vendor personnel who can answer detailed questions about specific portions of the product. The evaluation team tests the product against each requirement, making any necessary interpretations of the criteria with respect to the product being evaluated.

The evaluation team writes a two-part final report on their findings about the system. The first part is publicly available (containing no proprietary information) and contains the overall class rating assigned to the system and the details of the evaluation team's findings when comparing the product against the evaluation criteria. The second part of the evaluation report contains vulnerability analyses and other detailed information supporting the rating decision. Since this part may contain proprietary or other sensitive information it will be distributed only within the U.S. Government on a strict need-to-know and non-disclosure basis, and to the vendor. No portion of the evaluation results will be withheld from the vendor.

APPENDIX B

Summary of Evaluation Criteria Divisions

The divisions of systems recognized under the trusted computer system evaluation criteria are as follows. Each division represents a major improvement in the overall confidence one can place in the system to protect classified and other sensitive information.

Division (D): Minimal Protection

This division contains only one class. It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

Division (C): Discretionary Protection

Classes in this division provide for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.

Division (B): Mandatory Protection

The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Divison (A): Verified Protection

This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation.

APPENDIX C

Summary of Evaluation Criteria Classes

The classes of systems recognized under the trusted computer system evaluation criteria are as follows. They are presented in the order of increasing desirablity from a computer security point of view.

Class (D): Minimal Protection

This class is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

Class (C1): Discretionary Security Protection

The Trusted Computing Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class (C2): Controlled Access Protection

Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Class (B1): Labeled Security Protection

Class (B1) systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

Class (B2): Structured Protection

In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non-protection-critical elements. The TCB interface is well-defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

Class (B3): Security Domains

The class (B3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

Class (A1): Verified Design

Systems in class (A1) are functionally equivalent to those in class (B3) in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. In keeping with the extensive design and development analysis of the TCB required of systems in class (A1), more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

APPENDIX D

Requirement Directory

This appendix lists requirements defined in "Department of Defense Trusted Computer System Evaluation Criteria" alphabetically rather than by class. It is provided to assist in following the evolution of a requirement through the classes. For each requirement, three types of criteria may be present. Each will be preceded by the word: NEW, CHANGE, or ADD to indicate the following:

NEW: Any criteria appearing in a lower class are superseded by the criteria that follow.

CHANGE: The criteria that follow have appeared in a lower class but are changed for this class. Highlighting is used to indicate the specific changes to previously stated criteria.

ADD: The criteria that follow have not been required for any lower class, and are added in this class to the previously stated criteria for this requirement.

Abbreviations are used as follows:

NR: (No Requirement) This requirement is not included in this class.

NAR: (No Additional Requirements) This requirement does not change from the previous class.

The reader is referred to Part I of this document when placing new criteria for a requirement into the complete context for that class.

Figure 1 provides a pictorial summary of the evolution of requirements through the classes.

Audit

C1: NR.

C2: NEW: The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

B1: CHANGE: For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object **and the object's security level**. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity **and/or object security level.**

ADD: The TCB shall also be able to audit any override of human-readable output markings.

B2: ADD: The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels.

B3: ADD: The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded.

A1: NAR.

Configuration Management

C1: NR.

C2: NR.

B1: NR.

B2: NEW: During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

B3: NAR.

A1: CHANGE: During **the entire life-cycle, i.e., during the design, development,** and maintenance of the TCB, a configuration management system shall be in place **for all security-relevant hardware, firmware, and software** that maintains control of changes to **the formal model,** the descriptive **and formal** top-level **specifications,** other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. Also available shall be tools, **maintained under strict configuration control,** for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

ADD: A combination of technical, physical, and procedural safeguards shall be used to protect from unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.

Covert Channel Analysis

C1: NR.

C2: NR.

B1: NR.

B2: NEW: The system developer shall conduct a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.)

B3: CHANGE: The system developer shall conduct a thorough search for **covert channels** and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel.

A1: ADD: Formal methods shall be used in the analysis.

Design Documentation

C1: NEW: Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

C2: NAR.

B1: ADD: An informal or formal description of the security policy model enforced by the TCB shall be available and an explanation provided to show that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model.

B2: CHANGE: **The** interfaces between **the TCB** modules shall be described. **A formal** description of the security policy model enforced by the TCB shall be available and **proven** that it is sufficient to enforce the security policy.

ADD: The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamperproof, cannot be bypassed, and is correctly implemented. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.)

B3: ADD: The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the DTLS. The elements of the DTLS shall be shown, using informal techniques, to correspond to the elements of the TCB.

A1: CHANGE: The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the **formal top-level specification (FTLS)**. The elements of the **FTLS** shall be shown, using informal techniques, to correspond to the elements of the TCB.

ADD: Hardware, firmware, and software mechanisms not dealt with in the FTLS but strictly internal to the TCB (e.g., mapping registers, direct memory access I/O) shall be clearly described.

Design Specification and Verification

C1: NR.

C2: NR.

B1: NEW: An informal or formal model of the security policy supported by the TCB shall be maintained that is shown to be consistent with its axioms.

B2: CHANGE: **A formal** model of the security policy supported by the TCB shall be maintained that is **proven** consistent with its axioms.

ADD: A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface.

B3: ADD: A convincing argument shall be given that the DTLS is consistent with the model.

A1: CHANGE: **The FTLS** shall be shown to be an accurate description of the TCB interface. A convincing argument shall be given that the DTLS is consistent with the model **and a combination of formal and informal techniques shall be used to show that the FTLS is consistent with the model.**

ADD: A formal top-level specification (FTLS) of the TCB shall be maintained that accurately describes the TCB in terms of exceptions, error messages, and effects. The DTLS and FTLS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface. This verification evidence shall be consistent with that provided within the state-of-the-art of the particular Computer Security Center-endorsed formal specification and verification system used. Manual or other mapping of the FTLS to the TCB source code shall be performed to provide evidence of correct implementation.

Device Labels

C1: NR.

C2: NR.

B1: NR.

B2: NEW: The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

B3: NAR.

A1: NAR.

Discretionary Access Control

C1: NEW: The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both.

C2: CHANGE: The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups **of individuals**, or by both.

ADD: The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

B1: NAR.

B2: NAR.

B3: CHANGE: The enforcement mechanism (**e.g., access control lists**) shall allow users to specify and control sharing of those **objects**. These access controls shall be capable of **specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object**.

ADD: Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given.

A1: NAR.

Exportation of Labeled Information

C1: NR.

C2: NR.

B1: NEW: The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the current security level associated with a single-level communication channel or I/O device.

B2: NAR.

B3: NAR.

A1: NAR.

Exportation to Multilevel Devices

C1: NR.

C2: NR.

B1: NEW: When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

B2: NAR.

B3: NAR.

A1: NAR.

Exportation to Single-Level Devices

C1: NR.

C2: NR.

B1: NEW: Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

B2: NAR.

B3: NAR.

A1: NAR.

Identification and Authentication

C1: NEW: The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user.

C2: ADD: The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

B1: CHANGE: Furthermore, the TCB shall **maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to**

authenticate the user's identity and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual user.

B2: NAR.

B3: NAR.

A1: NAR.

Label Integrity

C1: NR.

C2: NR.

B1: NEW: Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

B2: NAR.

B3: NAR.

A1: NAR.

Labeling Human-Readable Output

C1: NR.

C2: NR.

B1: NEW: The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

B2: NAR.

B3: NAR.

A1: NAR.

Labels

C1: NR.

C2: NR.

B1: NEW: Sensitivity labels associated with each subject and storage object under its control (e.g., process, file, segment, device) shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

---

* The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

B2: CHANGE: Sensitivity labels associated with each **ADP system resource (e.g., subject, storage object) that is directly or indirectly accessible by subjects external to the TCB** shall be maintained by the TCB.

B3: NAR.

A1: NAR.

Mandatory Access Control

C1: NR.

C2: NR.

B1: NEW: The TCB shall enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between subjects and objects controlled by the TCB: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level.

B2: CHANGE: The TCB shall enforce a mandatory access control policy over all **resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB**. The following requirements shall hold for all accesses between **all subjects external to the TCB and all objects directly or indirectly accessible by these subjects**:

B3: NAR.

A1: NAR.

Object Reuse

C1: NR.

C2: NEW: When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

B1: NAR.

B2: NAR.

B3: NAR.

A1: NAR.

Security Features User's Guide

C1: NEW: A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

C2: NAR.

B1: NAR.

B2: NAR.

B3: NAR.

A1: NAR.

Security Testing

C1: NEW: The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. (See the Security Testing guidelines.)

C2: ADD: Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

B1: NEW: The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. All discovered flaws shall be removed or neutralized and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. (See the Security Testing Guidelines.)

B2: CHANGE: All discovered flaws shall be **corrected** and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced.

ADD: The TCB shall be found relatively resistant to penetration. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification.

B3: CHANGE: The TCB shall be **found resistant to** penetration.

ADD: No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain.

A1: CHANGE: Testing shall demonstrate that the TCB implementation is consistent with the **formal** top-level specification.

ADD: Manual or other mapping of the FTLS to the source code may form a basis for penetration testing.

Subject Sensitivity Labels

C1: NR.

C2: NR.

B1: NR.

B2: NEW: The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

B3: NAR.

A1: NAR.

System Architecture

C1: NEW: The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

C2: ADD: The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

B1: ADD: The TCB shall maintain process isolation through the provision of distinct address spaces under its control.

B2: NEW: The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified.

B3: ADD: The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.

A1: NAR.

System Integrity

C1: NEW: Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

C2: NAR.

B1: NAR.

B2: NAR.

B3: NAR.

A1: NAR.

Test Documentation

C1: NEW: The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing.

C2: NAR.

B1: NAR.

B2: ADD: It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths.

B3: NAR.

A1: ADD: The results of the mapping between the formal top-level specification and the TCB source code shall be given.

Trusted Distribution

C1: NR.

C2: NR.

B1: NR.

B2: NR.

B3: NR.

A1: NEW: A trusted ADP system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures (e.g., site security acceptance testing) shall exist for assuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies.

Trusted Facility Management

C1: NR.

C2: NR.

B1: NR.

B2: NEW: The TCB shall support separate operator and administrator functions.

B3: ADD: The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

A1: NAR.

Trusted Facility Manual

C1: NEW: A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

C2: ADD: The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

B1: ADD: The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner.

B2: ADD: The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described.

B3: ADD: It shall include the procedures to ensure that the system is initially started in a secure manner. Procedures shall also be included to resume secure system operation after any lapse in system operation.

A1: NAR.

Trusted Path

C1: NR.

C2: NR.

B1: NR.

B2: NEW: The TCB shall support a trusted communication path between itself and user for initial login and authentication. Communications via this path shall be initiated exclusively by a user.

B3: CHANGE: The TCB shall support a trusted communication path between itself and **users for use when a positive TCB-to-user connection is required (e.g., login, change subject security level).** Communications via this **trusted** path shall be **activated** exclusively by a user **or the TCB and shall be logically isolated and unmistakably distinguishable from other paths.**

A1: NAR.

Trusted Recovery

C1: NR.

C2: NR.

B1: NR.

B2: NR.

B3: NEW: Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.

A1: NAR.

(this page is reserved for Figure 1)

GLOSSARY

Access - A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Approval/Accreditation - The official authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

Audit Trail - A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

Authenticate - To establish the validity of a claimed identity.

Automatic Data Processing (ADP) System - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Bandwidth - A characteristic of a communication channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second.

Bell-LaPadula Model - A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving that the system is secure. A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode. The clearance/classification scheme is expressed in terms of a lattice. See also: Lattice, Simple Security Property, *-Property.

Certification - The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Channel - An information transfer path within a system. May also refer to the mechanism by which the path is effected.

Covert Channel - A communication channel that allows a process to transfer information in a manner that violates the system's security policy. See also: Covert Storage Channel, Covert Timing Channel.

Covert Storage Channel - A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel - A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

Data - Information with a specific physical representation.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Descriptive Top-Level Specification (DTLS) - A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Domain - The set of objects that a subject has the ability to access.

Dominate - Security level S_1 is said to dominate security level S_2 if the hierarchical classification of S_1 is greater than or equal to that of S_2 and the non-hierarchical categories of S_1 include all those of S_2 as a subset.

Exploitable Channel - Any channel that is useable or detectable by subjects external to the Trusted Computing Base.

Flaw Hypothesis Methodology - A system analysis and penetration technique where specifications and documentation for the system are analyzed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw actually exists and, assuming a flaw does exist, on the ease of exploiting it and on the extent of control or compromise it would provide. The prioritized list is used to direct the actual testing of the system.

Flaw - An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed.

Formal Proof - A complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems. The formal verification process uses formal proofs to show the truth of certain properties of formal specification and for showing that computer programs satisfy their specifications.

Formal Security Policy Model - A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a TCB, the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include: state transition models, temporal logic models, denotational semantics models, algebraic specification models. An example is the model described by Bell and LaPadula in reference [2]. See also: Bell-LaPadula Model, Security Policy Model.

Formal Top-Level Specification (FTLS) - A Top-Level Specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven.

Formal Verification - The process of using formal proofs to demonstrate the consistency (design verification) between a formal specification of a system and a formal security policy model or (implementation verification) between the formal specification and its program implementation.

Functional Testing - The portion of security testing in which the advertised features of a system are tested for correct operation.

General-Purpose System - A computer system that is designed to aid in solving a wide variety of problems.

Lattice - A partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound.

Least Privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mandatory Access Control - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

Multilevel Device - A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

Multilevel Secure - A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

Object Reuse - The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media must contain no residual data from the previously contained object(s).

Output - Information that has been exported by a TCB.

Password - A private character string that is used to authenticate an identity.

Penetration Testing - The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users.

Process - A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.

Protection-Critical Portions of the TCB - Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects.

Protection Philosophy - An informal description of the overall design of a system that delineates each of the protection mechanisms employed. A combination (appropriate to the evaluation class) of formal and informal techniques is used to show that the mechanisms are adequate to enforce the security policy.

Read - A fundamental operation that results only in the flow of information from an object to a subject.

Read Access - Permission to read information.

Reference Monitor Concept - An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Resource - Anything used or consumed while performing a function. The categories of resources are: time, information, objects (information containers), or processors (the ability to use information). Specific examples are: CPU time; terminal connect time; amount of directly-addressable memory; disk space; number of I/O requests per minute, etc.

Security Kernel - The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Level - The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model - An informal presentation of a formal security policy model.

Security Testing - A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also: Functional Testing, Penetration Testing, Verification.

Sensitive Information - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Sensitivity Label - A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.

Simple Security Property - A Bell-LaPadula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

Single-Level Device - A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, sensitivity labels do not have to be stored with the data being processed.

***-Property (Star Property)** - A Bell-LaPadula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. Also known as the Confinement Property.

Storage Object - An object that supports both read and write accesses.

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

Subject Security Level - A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user the subject is associated with.

TEMPEST - The study and control of spurious electronic signals emitted from ADP equipment.

Top-Level Specification (TLS) - A non-procedural description of system behavior at the most abstract level. Typically a functional specification that omits all implementation details.

Trap Door - A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g., special "random" key sequence at a terminal).

Trojan Horse - A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the Trojan Horse.

Trusted Computer System - A system that employs sufficient hardware and software integrity measures to allow its use for processing sensitive information.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Path - A mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software.

Trusted Software - The software portion of a Trusted Computing Base.

User - Any person who interacts directly with a computer system.

Verification - The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, TLS with source code, or source code with object code). This process may or may not be automated.

Write - A fundamental operation that results only in the flow of information from a subject to an object.

Write Access - Permission to write an object.

REFERENCES

1. Anderson, J. P. Computer Security Technology Planning Study, ESD-TR-73-51, vol. I, ESD/AFSC, Hanscom AFB, Bedford, Mass., October 1972 (NTIS AD-758 206).

2. Bell, D. E. and LaPadula, L. J. Secure Computer Systems: Unified Exposition and Multics Interpretation, MTR-2997 Rev. 1, MITRE Corp., Bedford, Mass., March 1976.

3. Brand, S. L. "An Approach to Identification and Audit of Vulnerabilities and Control in Application Systems," in Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, Z. Ruthberg, ed., NBS Special Publication #500-57, MD78733, April 1980.

4. Brand, S. L. "Data Processing and A-123," in Proceedings of the Computer Performance Evaluation User's Group 18th Meeting, C. B. Wilson, ed., NBS Special Publication #500-95, October 1982.

5. Denning, D. E. "A Lattice Model of Secure Information Flow," in Communications of the ACM, vol. 19, no. 5 (May 1976), pp. 236-243.

6. Denning, D. E. Secure Information Flow in Computer Systems, Ph.D. dissertation, Purdue Univ., West Lafayette, Ind., May 1975.

7. DoD 5200.1-R, Information Security Program Regulation, August 1982.

8. DoD Directive 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems, revised April 1978.

9. DoD 5200.28-M, ADP Security Manual -- Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, revised June 1979.

10. DoD Directive 5215.1, Computer Security Evaluation Center, 25 October 1982.

11. DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, January 1983.

12. DoD 5220.22-R, Industrial Security Regulation, January 1983.

13. DoD Directive 5400.11, Department of Defense Privacy Program, 9 June 1982.

14. Executive Order 12356, *National Security Information*, 6 April 1982.

15. Faurer, L. D. "Keeping the Secrets Secret," in *Government Data Systems*, November - December 1981, pp. 14-17.

16. Federal Information Processing Standards Publication (FIPS PUB) 39, *Glossary for Computer Systems Security*, 15 February 1976.

17. Federal Information Processing Standards Publication (FIPS PUB) 73, *Guidelines for Security of Computer Applications*, 30 June 1980.

18. Lampson, B. W. "A Note on the Confinement Problem," in *Communications of the ACM*, vol. 16, no. 10 (October 1973), pp. 613-615.

19. Lee, T. M. P., et al. "Processors, Operating Systems and Nearby Peripherals: A Consensus Report," in *Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls*, Z. Ruthberg, ed., NBS Special Publication #500-57, MD78733, April 1980.

20. Lipner, S. B. *A Comment on the Confinement Problem*, MITRE Corp., Bedford, Mass.

21. Millen, J. K. "An Example of a Formal Flow Violation," in *Proceedings of the IEEE Computer Society 2nd International Computer Software and Applications Conference*, November 1978, pp. 204-208.

22. Millen, J. K. "Security Kernel Validation in Practice," in *Communications of the ACM*, vol. 19, no. 5 (May 1976), pp. 243-250.

23. Nibaldi, G. H. *Proposed Technical Evaluation Criteria for Trusted Computer Systems*, MITRE Corp., Bedford, Mass., M79-225, AD-A108-832, 25 October 1979.

24. Nibaldi, G. H. *Specification of A Trusted Computing Base, (TCB)*, MITRE Corp., Bedford, Mass., M79-228, AD-A108-831, 30 November 1979.

25. OMB Circular A-71, Transmittal Memorandum No. 1, *Security of Federal Automated Information Systems*, 27 July 1978.

26. OMB Circular A-123, *Internal Control Systems*, 5 November 1981.

27. Ruthberg, Z. and McKenzie, R., eds. Audit and Evaluation of Computer Security, in NBS Special Publication #500-19, October 1977.

28. Schaefer, M., Linde, R. R., et al. "Program Confinement in KVM/370," in Proceedings of the ACM National Conference, October 1977, Seattle.

29. Schell, R. R. "Security Kernels: A Methodical Design of System Security," in Technical Papers, USE Inc. Spring Conference, 5-9 March 1979, pp. 245-250.

30. Trotter, E. T. and Tasker, P. S. Industry Trusted Computer Systems Evaluation Process, MITRE Corp., Bedford, Mass., MTR-3931, 1 May 1980.

31. Turn, R. Trusted Computer Systems: Needs and Incentives for Use in government and Private Sector, (AD # A103399), Rand Corporation (R-28811-DR&E), June 1981.

32. Walker, S. T. "The Advent of Trusted Computer Operating Systems," in National Computer Conference Proceedings, May 1980, pp. 655-665.

33. Ware, W. H., ed., Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, AD # A076617/0, Rand Corporation, Santa Monica, Calif., February 1970, reissued October 1979.

Mr. **Klein**. Second is to evaluate vendor products against these criteria and publish a listing for general use. This is an evaluated products list. I have some examples of bulletins of ongoing evaluations of commercial vendor products that we have evaluated against these criteria. They were evaluated while the criteria was still being developed, but really against the essence and the background of these criteria.

Third, the Center assists defense acquisition authorities in specifying and certifying trusted products that are used in defense systems.

And fourth, in conjunction with DOD components we formulate and sponsor research to improve the state-of-the-art in trusted-system technology and verification tools and methodologies.

And last, to strengthen the computer security awareness and confidence in the national security establishment, we engage in conducting specialized training, seminars—the one previously referred to in November is a jointly sponsored seminar by the Center and National Bureau of Standards and the Department of Defense, and information dissemination on our evaluation resources.

Let me define, what I mean by a trusted system. It is those systems, those ADP systems, that employ sufficient hardware and software measures to allow their use to simultaneously process a range of sensitive or classified information.

In the Department of Defense this means the classification headings, confidential, for example, through top secret. They could equally be applied, and they are applied, in the private sector for company proprietary information.

These trusted systems are to couple resources handling information spanning a range of sensitive classification levels to a diverse set of users without violating access privileges or compromising the information stored therein or handled therein.

As you know, this is a critical function in modern defense operations. That is to reliably handle sensitive data in electronic form in a time sensitive manner. Similar situations exist in a civil community regarding access to proprietary data in commerce and to government records on its citizens to which trusted computer technology could also be employed.

A recent article in the Computer World, the October 10 issue, addresses this subject very well, by Mr. Robert Campbell.

I would now like to turn my attention to how NSA activities in the communications security area can affect the civil community, and that is our participation with the Bureau of Standards in the development and deployment of the data encryption standard.

I believe that most of the testimony that I wanted to give on this subject has been covered by a previous witness but I will state with respect to the utilization of DES that in cooperation—or at the request, as was previously testified to—of the National Bureau of Standards, the National Security Agency did evaluate the data encryption standard for the purposes for which it was intended.

Admiral Bobby R. Inman, in 1979, issued a letter on endorsing NBS, and I would like to quote in part from that letter:

> ·NSA fully certified the Data Encryption Standard implemented by the Department of Commerce in July 1977, as a standard for the encryption of unclassified computer data . . . NSA will now endorse the use of the DES for encryption of unclassified national security-related information.

Additional efforts are underway since that time between the government and the industrial sector to introduce DES products to meet government needs and the protection of unclassified information.

Standards have now been issued for this purpose by the Federal Government. Domestic manufacturers may now submit DES-based equipments to NSA for evaluation against this standard. NSA will formally endorse those equipments that meet the Federal standard in question, that is FS1027.

This program is operating very successfully with over 20 manufacturers of DES products participating. A direct result of this process is a rapidly growing set of endorsed commercially available equipments available in the United States to meet both national security related and private sector telecommunications protection needs.

Let me turn my attention now to another topic, a question that was posed for our testimony with regard to voluntary review of research papers in the area of cryptography.

In 1979, Admiral Inman made a public address about articles and monographs on cryptography. While he recognized a growing need for cryptography in the public sector, he believed that uncontrolled publication of cryptographic papers could be harmful to the foreign intelligence and communications security missions of the National Security Agency.

In response to this concern, the American Council of Education, through a National Science Foundation grant, sponsored a study group to review the issues.

That group was composed of members of various professional organizations and technical societies; the IEEE and the Association for Computing Machinery among them, and also the NSA General Counsel.

In 1981, the group issued a report calling for prepublication review and laid down the conditions for those actions.

I want to point out that this was and is a voluntary process and in order to resolve disputes the group recommended an NSA established and advisory committee composed of three members recommended by the President's science adviser and two by the Director of NSA.

NSA has reviewed over a 100 papers and we have met our turn around time of getting word back to the office within 30 days 90 pecent of the time.

There have been disputes in three cases about the contents of the papers, and minor discussions with other content of the paper and all these situations were resolved without having to refer them to the special advisory committee.

Now I would like to turn to cryptographic research sponsored by NSA that would be of benefit to the civil community. A program was initiated several years ago in NSA to provide grants to university researchers in carrying out basic research related to cryptology.

This program has had a beneficial impact on our relationship with academe in that it has provided an excellent forum between the academics and NSA researchers, it has produced quality research of potential interest to NSA, and it has helped stimulate young scientists for future prospective recruitment.

The needs for future computer security research, these are being undertaken by the DOD computer Security Center.

I think some examples of future research in computer security that will benefit not only the DOD but the civil community as well on the areas of artificial intelligence, security modeling, proofs of correctness, all leading to secure operating systems which we believe is a vital link in electronic information protection and security.

This research is being performed by the Government in our laboratories in the academic sector and in private industry. The Center is playing a catalytic role in bringing the researchers together to meet these objectives.

We feel that the side benefits, and some that may be of primary benefit to this research is not only for security but for software reliability, computer availability, and also in super computer designs of the future.

Since the private sector will continue to be the prime source, I believe, of computer hardware and software and operating systems used by the Defense Department and the private sector, we feel it is imperative that security considerations for products to the private sector is going to provide to the Federal Government built-in security as an essential part and we are working with them to this end.

In the area of future communications security research, I would offer the following: The rapid expansion in use of communications throughout the Government, and the many new types of systems being introduced presents a significant challenge to our ability to provide adequate protection technology in the future. Some examples of this are cellular radio, electronic mail, local area networks, and direct termination, are a few important examples of how communications technology will find increased use in both the government and private sectors.

The amount of research and development resources directed at meeting these challenges in the private sector must be expanded to meet Federal needs for these services with respect to areas in which NSA can make contributions to our society's general need for security and privacy in the future.

I believe that NSA can continue to make significant contributions to society's general need for security and privacy through its programs in fostering security awareness, good security practice and administrative controls, selected transfer of computer and communications security technology to the private sector in the civil community.

We are placing great emphasis on the fact that much of the computer security technology of interest to Defense is also applicable to a much larger public and private market in privacy of electronic records, computer fraud, crime and abuse, and as a counter to potential terrorist activities.

We are thus encouraging computer vendors to apply this technology to their future computer products so that we in DOD can reap the benefits.

This concludes my statement. I will be pleased to answer any questions you may have.

[The prepared statement of Mr. Klein follows:]

STATEMENT ON
TELECOMMUNICATIONS SECURITY AND PRIVACY

PRESENTED BY
MR. MELVILLE H. KLEIN
DIRECTOR, DOD COMPUTER SECURITY CENTER
NATIONAL SECURITY AGENCY

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
COMMITTEE ON SCIENCE AND TECHNOLOGY
U. S. HOUSE OF REPRESENTATIVES

ON
OCTOBER 17, 1983

INTRODUCTION

Mr. Chairman and members of the Subcommittee, I am pleased to have this opportunity to appear before you today to address NSA research activities relevant to your examination of security and privacy in the civil community.

Since the activities of the NSA are for the most part of a classified nature, my remarks are directed at those unclassified aspects of computer and telecommunications protection that can influence the directions taken outside the national security arena.

Over the past decade interest in information protection and privacy has spread with the rapid and pervasive use of computers in almost every facet of our every day lives. Efforts to counter the threats to privacy of citizens and the confidentiality of business and non-national security government information were undertaken by the private sector and civil agencies (NBS). I would like to address how these activities have benefited from the computer security and communications security research programs at NSA. First I will review the origin, purpose and operation of the DoD Computer Security Center.

PURPOSE AND OPERATION OF THE DOD COMPUTER SECURITY CENTER

The Center is an outgrowth of the DoD Computer Security Initiatives Consortium formed in 1978 under the Assistant Secretary of Defense for Command, Control and Intelligence to coordinate on-going computer security research within the Department. In January of 1981, the Deputy Secretary of Defense assigned to the Director of NSA, certain responsibilities for computer security within the DoD. The Center began operation in June of 1981 as a separate and unique entity within the NSA. Its implementing directive (DoD Directive 5215.1) was issued by the Deputy Secretary of Defense in October 1982.

The Center has a five-pronged mission. First, to develop and promulgate uniform computer security criteria and standards that will lead to widespread availability of "trusted" products from computer vendors (Computer Security Evaluation Criteria). Second, to evaluate vendor products against these criteria and publish a listing for general use (Evaluated Products List). Third, to assist defense acquisition authorities in specifying and certifying trusted products in defense systems. Fourth, in conjunction with the DoD components to formulate and sponsor research to improve the state-of-the-art in trusted computer technology and verification tools and methodologies. And, lastly, to strengthen the computer security awareness and competence in the national security establishment through specialized training, seminars, information dissemination and ready access to evaluation resources.

By "trusted" computer systems, I mean those that employ sufficient hardware and software measures to allow their use to simultaneously process a range of sensitive or classified information (e.g. Confidential through Top Secret) for a diverse set of users without violating access privileges. This is a critical function in modern defense operations, i.e., reliably handling sensitive data in electronic form in a time-sensitive manner. Similar situations exist in the civil community regarding access to proprietary data in commerce and to government records on citizens to which trusted computer technology could also be employed.

NSA ACTIVITIES IN THE COMMUNICATIONS AREA THAT AFFECT THE CIVIL COMMUNITY

I would now like to discuss our participation in the development of the Data Encryption Standard (DES). The DES was proposed by the National Bureau of Standards as a means for protecting unclassified Government data in computers. The cryptographic algorithm was derived as a result of a 1973 solicitation to the Industrial Community. The algorithm selected was one proposed by the International Business Machines Corporation. It was extensively analyzed in several public workshops as well as by the National Security Agency at the request of the NBS. Admiral B. R. Inman, then Director of NSA, issued this endorsement of DES in a June 1978 letter:

"...NSA fully certified the Data Encryption Standard implemented by the Department of Commerce in July 1977, as a standard for the encryption of unclassified computer data...NSA will now endorse the use of the DES for encryption of unclassified national security-related information..."

Additional efforts are underway between the Government and the industrial sector to introduce DES products to meet Government needs for the protection of unclassified information.

Standards have now been issued for this purpose by the Federal Government (Federal Standard 1027). Domestic manufacturers may now submit DES-based equipments to NSA for evaluation against this standard. NSA will formally endorse those equipments that meet FS1027. This program is operating very successfully with over 20 manufacturers of DES products participating. A direct result of this process is a rapidly growing set of endorsed commercially available equipments available in the U.S. to meet both national security related and private sector telecommunications protection needs.

VOLUNTARY REVIEW OF RESEARCH PAPER

In 1979 Admiral Inman spoke out publicly about articles and monographs written on cryptography. While he recognized the growing need for cryptography in the public sector, he believed that uncontrolled publication of cryptographic papers could be harmful to the foreign intelligence and COMSEC missions of the NSA. In response to this concern, the American Council of Education, through a National Science Foundation grant, sponsored a study group to review the issues.

That Group, the Public Cryptography Study Group, was composed of members of various professional organizations and technical societies (e.g., IEEE and its Association for Computing Machinery) and NSA's General Counsel. In 1981 the Group issued a report calling for a system for voluntary pre-publication review. NSA, in complying with the recommendations of the report, issued an invitation to authors, Professional Societies and publications to submit manuscripts for pre-publication review. This invitation was also placed in the Federal Register in March 1982. The Study Group recommended, and NSA established, an advisory committee to resolve disputes that might arise between NSA and authors over the security implications of a paper. The Committee is composed of three members recommended by the President's Science Advisor and two by the Director, NSA. There has never been a need for it to meet.

It is important to point out that this is a voluntary process. We at NSA believe it is working to the mutual satisfaction of all parties. We have reviewed over 100 papers. Our stated objective is to staff and respond to these papers within 30 days. We have met this goal on over 90% of the cases.

Only a handful have raised some security concerns with our reviewers. Several of those were resolved with only minor modification to the text. We have asked that three papers not be published. In all of these situations the authors were most cooperative.

There was concern by some in the A.C.E. Study Group that a review procedure would have a "chilling effect" on research. I don't believe this has been the case. Our reviews are timely and responsive to the author's concerns.

Needs for Future Research in OCREAE PROGRAM

The OCREAE program is a small grant program operated by NSA to provide University researchers support for carrying out basic research related to Cryptology. This program has had beneficial impact on the NSA-academe relationship in that it has provided an excellent liaison mechanism between the academics and NSA researchers, it has produced quality research of potential interest to NSA, and it has helped create a source of talented young scientists for prospective recruitment.

Needs for Future Computer Security Research

Some examples of the types of research needed in the future that will benefit computer security are in the areas of artificial intelligence, security modeling, proofs of correctness, and secure operating systems. This research is being performed by the government, academia, and private industry, and is expected to expand not only to meet our needs but those of others in software reliability and supercomputer design.

Needs for Future Communications Security Research

The rapid expansion in the use of communications throughout the government, and the many new types of systems being introduced, presents a significant challenge to the ability to provide adequate protection technology in the future. Cellular radio, electronic mail, local area networks, and direct termination systems are but a few examples of the new communications technology which will find increased use in both the Government and private sectors. The amount of research and development resources directed at meeting these challenges in the private sector needs to be expanded.

Areas in Which NSA Can Make Contributions to Our Society's General Need for Security and Privacy in the Future

We believe that NSA can continue to make significant contributions to our society's general need for security and privacy through its programs of security awareness, good security practice and administrative controls, and continued selective technology transfer from our on-going communications security research to the private and public sectors. We are placing emphasis on the fact that much of the computer security technology of interest to defense is also applicable to a much larger public and private market in privacy of electronic records, computer fraud, crime and abuse, and as a counter to potential terrorist activity. We are thus encouraging computer vendors to apply this technology to their future computer products so that we in DoD can also reap the benefits.

This concludes my statement. I will be pleased to try and answer any questions that you may have.

Mr. GLICKMAN. Thank you very much, Mr. Klein.

Does NSA have difficulty recruiting experts in computer security?

Mr. KLEIN. Not as much as I thought I was going to have when I took this position about 18 months ago. We currently have over 100 people; four-fifths of them are technical, in the Center, on computer security. I think we offer an attractive working environment in the Center and very interesting technical challenges.

Mr. GLICKMAN. So there is no people power shortage, then, in the area?

Mr. KLEIN. I said there was not as much as I expected but we are still below critical mass; we would like to increase our numbers by a factor of two in the next 2 fiscal years. We are authorized to do that.

Mr. GLICKMAN. OK.

Mr. KLEIN. I think that the universities are swamped with more applications for computer security than they can handle at this point in time. We are competing fairly well with industry in getting computer scientists into the Center.

Mr. GLICKMAN. On page 2 of your statement you talk about the Center having a five-prong mission, and you mention the five missions of the DOD Computer Center.

Are the results of your work, for example, the evaluated products list, as well as the others, available to private sector users?

Mr. KLEIN. Yes; they are.

Mr. GLICKMAN. In what form?

Mr. KLEIN. I have some examples of an evaluation bulletin that describes the product and describes how it stacks up to our criteria which I would be happy to leave with you.

Mr. GLICKMAN. Why don't you? That would be useful to us.

I mean, do you wait for them to ask for the input or do you provide it on an ongoing basis?

Mr. KLEIN. If they are on our mailing list we will provide them if there is an interest expressed in a particular type of product, if it is accessed in full, secure auditing, whatever the situation might be.

Mr. GLICKMAN. Also on page 2 you refer to evaluation of computers. I think you indicated that you would supply us for the record the criteria you use in the evaluation of computers.

Mr. KLEIN. Yes, sir.

Mr. GLICKMAN. OK.

Mr. KLEIN. I have a copy of that.

Mr. GLICKMAN. Yes; we would appreciate that very much.

[The bulletin follows:]

DoD COMPUTER SECURITY CENTER
9800 Savage Road
Fort George G. Meade, Maryland 20755

PRODUCT EVALUATION BULLETIN*

Report No. CSC-PB-01-83

AS OF: 15 April 1983

PRODUCT: Secure Communications Processor (SCOMP)

VENDOR: HONEYWELL Information Systems, Inc.

DESCRIPTION:

The SCOMP hardware consists of a standard HONEYWELL Level 6/DPS 6 minicomputer with a modified CPU, and to which a Security Protection Module (SPM) has been added. The SPM provides segmentation, paging, protection rings similar to the HONEYWELL Level 68 Multics, with argument validation, and virtual address translation for I/O programs and devices.

The primary software security mechanism of the SCOMP system is the security kernel, based on the Bell-LaPadula model of the DoD security policy, which provides a foundation on which to build dedicated secure applications programs. The SCOMP Kernel Interface Package (SKIP) and Trusted Software (a set of security-relevant, non-kernel code) provide a basic terminal-oriented operating system interface that runs on, and derives its security from, the security kernel. SKIP includes a hierarchical file system and a process structure which supports the dynamic creation and destruction of processes. Trusted Software includes user, maintenance, and operator services.

SCOMP software is supported by Honeywell Federal Systems Division in McLean, VA, and the hardware is supported by Honeywell Small Systems and Peripheral Division in Billerica, MA.

---

*The DoD Computer Security Center maintains and publishes an Evaluated Products List (EPL) of selected industry and government developed trusted computer systems and computer products in a manner suitable for use by the National Security Establishment and the Department of Defense. The Center issues Product Evaluation Bulletins to provide the status on the products currently under evaluation.

STATUS:

The development of the SCOMP hardware has been sponsored by the Naval Electronics System Command (NAVELEX) under the auspices of the DoD Computer Security Initiative Program. As of this writing, the system has been delivered to six test sites, and is under active consideration for several operational environments (e.g., FORSCOM GUARD). The currently existing software support includes a Level 6/DPS 6 C compiler, a Level 6/DPS 6 Assembler, an Editor, a Linker, and a set of program development utilities. A UNIX* environment for the system is presently being implemented by Honeywell, which is scheduled for completion by the end of 1983. A general purpose network interface has been provided through an ARPANET 1822 Network Interface Adapter and the implementation of the Transmission Control Protocol (TCP-4).

SECURITY EVALUATION STATUS:

The formal evaluation of the Honeywell SCOMP is presently in progress. The evaluation team was formed and the formal effort commenced in August 1982, with completion scheduled for 4Q FY83. The product is being evaluated against the final draft of the Trusted Computer System Evaluation Criteria, dated 27 January 1983, and is considered to be a candidate for the A1 evaluation class. At this point, all the formal specification and verification of the kernel design has been completed, and the majority of the evidence and documentation required to complete the evaluation have been submitted by the vendor. The major item awaiting completion at this time is the documentation of the formal top-level specifications for the Trusted Software. This work is currently being funded under the NAVELEX contract.

ENVIRONMENTAL STRENGTHS:

The advantages of the SCOMP system derive from the hardware support provided for security-related processing requirements, and from enhancements designed with the goal of maintaining performance for secure processing. The product was originally targetted for general purpose, multi-level secure, time-sharing applications. While the underlying system was designed to support such an environment, the currently available applications-support software (SKIP and Trusted Software) provide a secure base upon which one may overlay specific applications. Although the formal evaluation is still in progress, it is clear at this point that the Honeywell SCOMP can provide a state-of-the-art base for a variety of security-sensitive applications. Thus, it should be considered an acceptable candidate for a wide range of minicomputer applications which demand an enhanced architecture to support requirements for secure processing, e.g., communications processor, GUARD applications, database systems, etc.

---

*UNIX is a trademark of Bell Laboratories.

DOD COMPUTER SECURITY CENTER
9800 Savage Road
Fort George G. Meade, Maryland 20755

PRODUCT EVALUATION BULLETIN*

Report No. CSC-PB-03-83

AS OF: 15 April 1983

PRODUCT: the Access Control Facility (ACF2)

VENDOR: SKK, Inc.

DESCRIPTION:

The ACF2 security subsystem is designed to provide security for data stored on computer systems using the IBM MVS or VS1 operating systems. ACF2 provides protection by default for data sets resident on Direct Access Storage Devices (DASD), IBM 3850 Mass Storage System (MSS) and Tape volumes. Protection levels of READ, WRITE, ALLOCATE (allocation, rename, scratch and catalog functions) and EXECUTE-only are supported.

Interfaces between ACF2 and many popular commercial software products are provided by SKK. These software products include Information Management System (IMS) and Customer Information Control System (CICS) by IBM.

STATUS:

ACF2 was developed by SKK, Inc. and is marketed by the Cambridge Systems Group. SKK provides product support and issues updates and enhancements as applicable. ACF2 is currently available from the vendor at the Release 3.1.3 software level.

---

*The DoD Computer Security Center maintains and publishes an Evaluated Products List (EPL) of selected industry and government developed trusted computer systems and computer products in a manner suitable for use by the National Security Establishment and the Department of Defense. The Center issues Product Evaluation Bulletins to provide the status on the products currently under evaluation.

SECURITY EVALUATION STATUS:

The formal evaluation of ACF2 Release 3.1.3 commenced in December 1982 and is scheduled for completion by the end of the third quarter of FY 83. ACF2 will be evaluated against the final draft of the DoD Trusted Computer System Evaluation Criteria dated 27 January 1983. The DoD Computer Security Center considers ACF2 a candidate for the class of products which provide discretionary protection (i.e., class C2). A formal evaluation report will be produced by the DoD Computer Security Center.

ENVIRONMENTAL STRENGTHS:

The advantages of the ACF2 security subsystem derive from the default protection of all data sets resident on DASD, MSS and Tape volumes. The numerous options selectable at installation time allow the implementor of ACF2 to tailor the product to provide a high level of discretionary security as an add-on package to the IBM MVS and VS1 operating systems. ACF2 provides extensive audit capability to the system security administrator via the IBM System Management Facility and ACF2 report utilities. These utilities allow the auditor to retrieve audit information on specific statistics.

DOD COMPUTER SECURITY CENTER
9800 Savage Road
Fort George G. Meade, Maryland 20755

PRODUCT EVALUATION BULLETIN*

Report No. CSC-PB-04-83

AS OF: 1 April 1983

PRODUCT: Multics

VENDOR: Honeywell Information Systems (HIS)

DESCRIPTION:

The Multics operating system runs on a large mainframe, the standard Honeywell Level 68/DPS or Honeywell DPS 8/70M computer. However, the CPU's were specifically designed for the Multics operating system, thereby providing hardware support for protection rings and segmentation.

Multics was designed to provide a good general purpose time-sharing environment to the typical user, and has typically been used in large-scale software development, relational database applications, network-oriented applications, and applications requiring unique security constraints.

Multics provides three basic security mechanisms. At the lowest level are the hardware supported protection rings and segmentation which provide tightly controlled and separate domains of execution. Next is the the Access Isolation Mechanism (AIM) which provides mandatory access control. Finally, at the level closest to the user, are the Access Control Lists (ACL's) which provide discretionary access control.

STATUS:

Multics was developed by MIT and HIS and first marketed in January 1973. It is marketed and supported by HIS, with version 10.1 being the latest available release.

---

*The DoD Computer Security Center maintains and publishes an Evaluated Products List (EPL) of selected industry and government developed trusted computer systems and computer products in a manner suitable for use by the National Security Establishment and the Department of Defense. The Center issues Product Evaluation Bulletins to provide the status on the products currently under evaluation.

SECURITY EVALUATION STATUS:

A formal evaluation of Multics ver. 10.1 started in December 1982 and is scheduled for completion in the fall of 1983. The Department of Defense Computer Security Center considers Multics as a candidate for a B2 level system. The evaluation will be completed using the 27 January 1983 draft of the Trusted Computer System Evaluation Criteria. The placement of Multics on the EPL will be based on this evaluation.

ENVIRONMENTAL STRENGTHS:

Multics provides eight hierarchical hardware supported protection rings and segment based addressing. These features provide very controlled and relatively efficient mechanisms for information sharing between processes. The AIM mechanism, coupled with the ACL's, gives the system a very flexible way to conform to the lattice model of the DoD security policy. Thus, since Multics supports the DoD security policy at the level of a full, general purpose operating system, it is a convenient base upon which to build specific applications for which security is a basic requirement. Multics also provides an environment capable of running existing user-level GCOS programs. In addition, there is a vendor supported network package that is compatible with the new ARPANET TCP protocol, including MAIL, FTP and TELNET. Multics also supports large relational databases and RPG.

Multics is written primarily in PL/1. This not only means system maintenance is easier but that the user interface to system routines is very friendly. Therefore, making it easy to write application code that makes use of Multics' unique security features as well as other system functions. The ring mechanism also gives one the ability to write very tightly controlled subsystems. For example, one could set-up a database that could only be accessed from specific programs, thereby allowing the type of very fine grain access control necessary for dealing with Privacy Act type information.

Multics has been used in large-scale software development environments. Because of Multics' unique protection facilities it has been often heralded as the model for other secure computer environments. Multics has been accredited to run in a two-level classified (secret/top-secret) timesharing mode at selected DoD installations since December 1976.

DOD COMPUTER SECURITY CENTER
9800 Savage Road
Fort George G. Meade, Maryland 20755

PRODUCT EVALUATION BULLETIN*

Report No. CSC-PB-02-83

AS OF: 15 April 1983

PRODUCT: Resource Access Control Facility (RACF)

VENDOR: IBM

DESCRIPTION:

RACF is IBM's MVS facility that provides controlled access to system resources. It is supported under MVS/370 and MVS/XA. RACF is designed to limit access to resources by identifying authorized users and protected resources, then controlling users' access to those resources. RACF also provides the security administrator with the option of default protection on permanent Direct Access Storage Device (DASD) data sets. RACF provides protection for data sets resident on DASD, IBM Mass Storage Systems (MSS) and Tape volumes. Access levels of NONE, READ, UPDATE, ALTER, and CONTROL are supported for DASD data sets.

Interfaces between RACF and other IBM products, including Information Management System (IMS) and Customer Information Control System (CICS), are supported by IBM.

STATUS:

RACF was developed and is marketed by IBM. IBM provides product support and issues updates and enhancements as applicable. RACF Version 1, Release 5 was released February 8, 1983.

---

*The DoD Computer Security Center maintains and publishes an Evaluated Products List (EPL) of selected industry and government developed trusted computer systems and computer products in a manner suitable for use by the National Security Establishment and the Department of Defense. The Center issues Product Evaluation Bulletins to provide the status on the products currently under evaluation.

SECURITY EVALUATION STATUS:

The formal evaluation of RACF Version 1, Release 5 commenced in November 1982 and is scheduled to be completed during the third quarter of FY 83. RACF will be evaluated against the final draft of the DoD Trusted Computer System Evaluation Criteria dated 27 January 1983. The DoD Computer Security Center considers RACF a candidate for the class of products which provide discretionary protection (i.e., class C2). A formal evaluation report will be produced by the DoD Computer Security Center.

ENVIRONMENTAL STRENGTHS:

The advantages of the RACF security subsystem derive from the option of default protection of all data sets resident on DASD. The numerous options selectable at installation time allow the implementor of RACF to tailor the product to provide a high level of discretionary security as an add-on subsystem to the IBM MVS operating system. RACF provides extensive audit capability to the system security administrator via the IBM System Management Facility and RACF report writing utilities. These utilities allow the auditor to retrieve audit information on specific access activities.

Mr. GLICKMAN. We very much appreciate your coming down here and testifying today. We believe this is a major national problem issue and your technical input is quite useful. Thank you very much.

Mr. KLEIN. Thank you.

Mr. GLICKMAN. Our next witness is from the FBI. We have Floyd Clarke, Inspector-Deputy Assistant Director of Criminal Investigation Division. And I hope I am saying this name right, Kier T. Boyd, Acting Assistant Director of the Technical Services Division of the FBI.

Mr. BOYD. Yes.

Mr. GLICKMAN. I hope I got the names right. If there is anybody else with you, you might indicate that. We appreciate your being here. Your statement is not very long so you may feel free to read it or summarize it as you deem appropriate.

Why don't you proceed?

STATEMENT OF FLOYD I. CLARKE, DEPUTY ASSISTANT DIRECTOR, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION, ACCOMPANIED BY KIER T. BOYD, ACTING ASSISTANT DIRECTOR, TECHNICAL SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION, AND ANTHONY J. ADAMSKI, JR., CHIEF, FINANCIAL CRIMES UNIT, FEDERAL BUREAU OF INVESTIGATION

Mr. CLARKE. Thank you, Mr. Chairman. I do have with me also, to my left, Tony Adamski, who is the Unit Chief of our Financial Crimes Unit in our White Collar Crime Section.

I appreciate, Mr. Chairman, the opportunity that you have provided for the FBI to present its views on the subject of telecommunications, security and privacy, and to respond to your specific areas of concern.

Prior to responding to your specific questions, I would like to point out three things that we in the FBI believe are key to understanding *the FBI's perspective on computer-related crimes.*

The first of these issues is that a computer is an instrumentality of some other form of traditional crime, for instance, theft or larceny. It is much like a gun, a knife, or a forger's pen.

The second issue is of a more academic nature, but nevertheless important in that there does not exist, at this time, one generally recognized and accepted definition as to what computer crime is. Therefore, we do not have an objective standard to measure the trends of computer-related crime.

Last, in the view of the FBI's current structure of management by program, rather than by case, there is no method in place now to observe the statistical dimensions of computer-related crime.

With that in mind, I would like to discuss the nature, extent, and dimensions of crimes involving computers and communications from the FBI's perspective.

As you are aware, there is no one agency at this time that has jurisdiction for computer-related crimes and very probably there cannot be because of the wide application of computers. The FBI's jurisdiction in computer-related crimes is derived from jurisdiction previously assigned to the FBIL by Congress or the Attorney General of the United States in the more traditional areas.

Generally speaking, the statutes most frequently used by the Department of Justice and the FBI to prosecute and investigate computer-related crimes are fraud by wire, interstate transportation of stolen property, bank fraud and embezzlement, destruction of Government property, and the theft of Government property.

However, computer-related crimes transcend all of the crime categories and jurisdictions, local, State, and Federal, again making it difficult to measure the trends in this type of crime.

Another problem that has been encountered is a reluctancy on the part of some businesses, especially those in the financial community, to report losses attributable to computer-related crimes in an attempt to avoid developing an image of fiscal insecurity.

Therefore, in the absence of a generally accepted definition of computer-related crime, coupled with the lack of a central repository for the statistics on computer-related crimes, it would appear that the answer to your question regarding the extent of computer-related crime is that no one knows for sure.

Since the early 1970's, the FBI has been involved in computer-related crime investigations, and since that time we have noted no dramatic increase in the number of these FBI investigations. Logic would indicate that with the ever increasing number of computers in use today, there ought to be a corresponding increase in computer-related crimes; however, we have no credible documentation to support this sort of conclusion.

As to the dimension of computer-related crimes, there is a large potential for extremely large losses. Most financial institutions, as well as our Government and governments of other countries, utilize computers to facilitate their operations. This creates a potential for abuse by persons who have the necessary knowledge, time and access to the correct hardware or software.

In a very short period of time, programs, high technology information, proprietary information or classified information can be taken from a computer without leaving much evidence of the crime. This is to say nothing of the theft of large amounts of money transferred by wire between financial institutions.

In your response—in response to your request for illustrations of computer-related crime that the FBI has been involved in, I would like to bring to your attention some specific instances of these types of crimes.

In 1979, the New York Division of the FBI identified a computer information service, which is a company that enters, edits, stores, and retrieves information in a text format, that was, without authorization, accessing and modifying records of a similar computer information service in the State of California.

The second computer service was the primary competitor of the first and the actions of the first computer service caused an estimated loss of $7.5 million.

In 1980, the New York Division again identified a group of children of middle school age who accessed without authorization, over 20 computers from the computer located at their school.

The unauthorized accesses by this group in both the United States and Canada not only caused the loss of computer time and disrupted computer services, but caused the destruction of inventory and billing figures of a Canadian firm. This necessitated substantial efforts by that firm to duplicate.

In late 1982, our Washington field office identified a former employer of the Federal Reserve bank who was then employed privately as a financial analyst, who attempted to continue to access information in the Federal Reserve bank's money one file without authorization. Any information he might have obtained from this file would have been useful in the analysis of his client's holdings.

Early in 1983, our office in Alexandria, Va., identified an individual who, without authorization, accessed computerized consumer credit information to obtain credit account information on over 80 people. Therefter he used this information to charge goods including additional computer equipment to the major credit cards of the people whose credit information he had accessed.

These examples are certainly not all inclusive of our efforts in computer-related crimes, but they give a broad view of the types of computer-related crimes that are presented to the FBI for investigation. We have so far been able to identify and locate the person or persons committing each of the beforementioned crimes. We hope to be able to continue to do so.

We in the FBI have not had, to date, any significant problems in prosecution of computer-related crime under already existing statutes over which we have jurisdiction, such as the fraud by wire statute.

Our experience indicates that certain legal issues involving computer-related crime could be clarified, particularly the definition of property in the sense of a computer program having its own clearly defined inherent value and also the issue of trespass.

Also, the most frequently heard defense for simple unauthorized access into someone else's computer is that the individual making the access has no criminal intent, meant no harm, there was no security system and, therefore, there is no trespass.

However, it is a fairly commonly held—it is fairly commonly held that if an individual without authorization enters the unlocked house of another and rummages through that person's closets with no intent to steal or do harm, that person could still be guilty of trespassing. It is important that a legal clarification be made in this regard.

In regard to preventive measures necessary to deal with computer-related crime it appears from our experience that this is more of a human problem than a technological one. In most instances where we have been involved in an investigation of computer-related crime the crime was perpetrated by someone who had access to the computer and authorization to use it. The crime was facilitated by the access and in most cases the authorization was exceeded or misused.

Finally, your staff requested that I address the need of law enforcement agencies for computer and communications security and privacy in their own operations.

It is a well documented fact that Government law enforcement agency radio communications are monitored by nonlaw enforcement elements, ranging from the hobbyist, who gains a vicarious thrill from being "in" on law enforcement operations, to the entrepreneur, who listens for profit; the news media or the person who markets lists of Government frequencies exhibiting interesting activity, to the criminal who listens to evade law enforcement operations as well as the foreign intelligence operative.

These elements monitor our radio circuits to gain information on our operations, through intercept and analysis of our radio traffic; to disrupt operations by learning of our movements in advance and evading or countering them; to identify and associate agents with the ongoing operations.

In short, we pay a severe penalty due to the vulnerability of our clear text voice radio systems used to control our operations.

We pay this penalty in terms of personnel overhead. Up to 20 percent of a surveillant's time may be spent to accommodate the verbal codes, additional surveillance vehicles, and other burdens imposed to protect those operations.

There are compromised cases, wherein hundreds of hours of effort may be wasted because the subject learned of our operations by monitoring our circuits and successfully evaded apprehension or, forewarned, was able to destroy vital evidence, thus jeopardizing prosecution.

There is a hazard to agents, agent identity, location or cover, and if compromised, it could place him in a highly dangerous position. Subjects have used intercepted radio transmissions to identify and endanger the life of operatives.

To counter the threat, voice protection measures must be applied to our radio system. In our counterintelligence operations, national defense is at stake and full speech security is required. In conducting our law enforcement operations; however, a significant deficiency exists in countering the known threat. In this area, speech security is not always warranted, but there is a distinct and pressing need for voice "privacy" on our radios nationwide.

Congress has recognized the critical need and has appropriated $64,600,000 in the FBI's 1984 budget for a voice privacy radio system. This money, combined with the funds appropriated in 1982 and 1983 will make our voice privacy system 70 percent complete.

Mr. Chairman, this concludes my prepared remarks and I would be happy to entertain any questions that you might have.

Mr. GLICKMAN. Thank you very much for an excellent statement.

You have listed four or five case studies of computer- or communications-related crimes. Is this meant to be an exclusive list of problems of investigations that you have conducted?

Mr. CLARKE. No, sir; it is not. That is only an example, and as I mentioned before, the fact that we do not keep a central repository of the types of crimes that you could define as computer-related. It is very difficult to give an extensive list. We have computers used in a wide range of different types of criminal activity. And under our current program management, each of those crimes would be collected and tabulated within the various programs.

Mr. GLICKMAN. Have you sensed a growing number of computer-related crimes affecting the Federal Government in the last few years—Social Security, Veterans' Administration, things where the financial status of, let's say, the citizen out there is affected?

Mr. CLARKE. The problem there is that we are not able to analyze any trends because there is no data base to compare it with. What we have done only recently is in our white collar crimes program we have attempted to segregate those crimes which could be defined as being computer-related, wherein the computer was either used as the instrumentality of the crime or where the computer was the target of the crime.

With the public awareness, with the expansions of use of computers, we do not believe that that is adequate either. And we are in the process of analyzing our various programs to develop a system whereby we will require each of our field offices to set up a control file identifying computer-related crimes that transcend all areas of our programs. And then on a periodic basis submit it to us at headquarters for an analysis. And, hopefully, by doing that we will be able to detect any trends in that regard.

Mr. GLICKMAN. OK, that's good to hear.

Now, we talked about this issue and this hearing is kind of precipitated by the use of unauthorized access to computers by the hackers in Milwaukee. It was quoted at the beginning of this hearing today that you had been involved in—recently—involving unaccessed, unauthorized access to other computer systems, just in the last 2 or 3 weeks, that you have been engaged in a fairly large investigation in this area.

Many of the young people involved in unauthorized or illegal access are not always aware that they are or have committed a crime. They are just playing a game. And others may have some knowledge that their impact into another system may cause some harm but they don't do it to steal anything.

Do you think that unauthorized access—I mean, well, first of all, let me ask you this question. Is the mere unauthorized access, the intentional unauthorized access into somebody else's computer, is that a crime under current law?

Mr. Clarke. Not necessarily. It is possible for an individual to gain access into a computer or into the system, and if there is no damage nor information acquired, that in and of itself would not constitute a Federal crime.

Mr. Glickman. When you talk about damage, what if there is no damage, but the invaded system has caused some degree of delays or costs in terms of getting their system back to where it was before. Would that constitute damage?

Mr. Clarke. Well, I think that's part of the problem that we need to look at in any legislation that may be addressed, the definition of the term damage. And also the—dealing with the concept of trespassing into a computer. I think as we were all growing up that our parents taught us that we should not go into the home of another even if the door was open and valuable property was lying there, even to look at that you—you were taught that that is something you shouldn't do. And there are in fact laws to preclude that kind of activity.

Right now the problem in the computer operations is that there is no law that precludes trespass. And it is extremely difficult unless there is damage or there is a theft to determine to what extent the owner of that property was harmed.

So I think the term damage and the issue of trespass are things that right now there is a void in the law.

Mr. Glickman. Have you ever found—you talk a little bit about that your voice communications or the protection of it—have you ever found any trespass into your own computers in terms of criminal data information stored on that?

Mr. Boyd. No, we haven't. On any system which the FBI has, we have National Security Agency equipment both at the end where the computer is operating, and out at the terminals. So anybody attempting to come in would have to get through that equipment. NSA, of course, assures us this cannot be done and we certainly found no evidence of anybody doing it.

Mr. Glickman. And is there any way that it could have been done without you knowing about it, or would the fingerprints or footprints been left, or do you know?

Mr. Boyd. Footprints would be there because all of our systems have what's called a log tape where we tape every transaction on the system and put it in a form which is retained for, I believe, 6 years.

Mr. Glickman. So—but, now there are people who obviously have access into your information base, local law enforcement agencies and the like, but they would have no capability—somebody who is working for them—to change information or——

Mr. Boyd. The office——

Mr. Glickman [continuing]. Or improperly get into the access in the first place?

Mr. Boyd. The only system that we have that's available outside the Bureau is the National Crime Information Center. Now, there if you wanted to gain information that was in that system, the easiest way would be to take somebody who now has lawful access to it and get him to get that information.

First of all, the information in that system at the present time is public source information so there is a question there as to protecting something which a person could go to a courthouse and get, for instance, the record of somebody's arrest.

Now, there are protections in that system; they are not of the same quality of the Bureau's internal system. For instance, we don't use National Security Agency type equipment or even privacy equipment. They do, however, use dedicated lines, any time a request is made it is a very highly structured format for the message.

So somebody would have to be familiar with the system to know how to use the identifier of the agency which is asking it, or at least their simulating that agency, and then be able to come in and access that particular data base. I believe that that would be possible but if somebody is that interested in getting the information it is much easier to go to somebody with lawful access and just get it from him.

Mr. Glickman. OK.

Have you—have you, yourself, assisted local law enforcement agencies in dealing with a lot of the problems we are talking about today, computer crime, unauthorized access, the whole variety of issues?

Mr. Clarke. Wherever our assistance has been sought we have responded, and in addition, we do have a—a training program that is offered for local Federal, State and local, and even foreign law enforcement. We have a 4-week school, which is now being presented in a condensed 3-week version, that is available for not only the FBI but State and local law enforcement. And we also have a 1-week program for familiarization with computer fraud and the terminology in environ—computer environment, that is presented on a road show basis where the instructors from Quantico travel out to the field and give instruction in that area.

Mr. Glickman. OK.

You briefly mentioned before that you were going to begin a data base on computer crime and that had not been done before.

Does that in any way relate to what the Department of Justice has established with—in a system called FACTS, Federal abuse and corruption tracking system?

Mr. Clarke. No, that is a separate system that was developed about a year ago, and this was to assist in the tracking of Government fraud cases only. Government fraud is only one of the three program areas—subprogram areas within our white collar crime program. So it would be restricted to only the Government fraud programs. And that is an off-line system that helps the Department of Justice as well as the IG community to track the—the prosecuting status of cases that are being handled within that program.

Mr. Glickman. OK.

What steps do you think can be taken, perhaps with the Bureau's help, to make the computer communication data base owner and user aware of the dangers of an unauthorized user in his system?

Mr. Clarke. I don't know what the FBI in and of itself can do other than through the investigation of the crimes that we have reported to us now, the corresponding publicity that is attendant to any prosecutive action related to that. And in the future if we are able to develop any meaningful statistics through our data collection efforts that would indicate any kind of trends or increases, that—publication of that kind of information would certainly be helpful.

Mr. GLICKMAN. OK.

What sort of—do you have any research efforts? Does the Bureau do any research into this area independent?

Mr. CLARKE. Well, our instructors at Quantico that do the lecturing try to keep abreast of the state-of-the-art technology and the problems that are being encountered through conversation with the agents and the local police officers who attend those various training seminars.

Mr. GLICKMAN. Have you had any reason to believe that the country suffers any danger from sabotage of major computer or communications systems? And is this part of the FBI's general investigatory concern?

I guess what I am talking about is that, you know, we have been talking about unauthorized access and all of the technological aspects. Well, I suppose through sabotage, either through foreign policy reasons or through financial purposes, one could intentionally damage computer systems to engage in a variety of activities either through traditional methods or through new technological methods, you know.

I wonder if—if this is on your agenda.

Mr. CLARKE. I would answer that in part and then I would like to defer to Mr. Boyd who may have something from their research and development aspects that technical services may be able to shed some light on.

But we are certainly sensitive to any intelligence information that we might receive that would deal with sabotage in any form, whether it be on a computer terminal or computer operation or whether it be through some other type of criminal activity. And we would certainly initiate whatever investigative steps were necessary to counter that.

We are not aware of—we do—we are not in the possession of any information that would indicate that there is any kind of that activity taking place.

As far as the vulnerability of our systems, as Mr. Boyd mentioned, the systems that we have that are on-line systems are protected with the state-of-the-art requirements for protecting that information and we are not aware of any trespass or attempt to trespass those—those systems.

I have no specific knowledge as to the type of security measures that are in place in other Government agencies and for that and any other I defer to——

Mr. BOYD. To the best of my knowledge of any system which processed national security information would be protected by NSA equipment. Now, there would be a level below that and it would go not just to Government but to firms in the private sector who were doing Government work. There, a particular system may well be vulnerable and not be protected either by full security or by privacy.

We have had, to the best of my knowledge—this is a little out of my realm because I am not on the investigative side—we have seen no attempt, that I am aware of, by a foreign government to exploit any such weakness. As far as people like hackers doing it, what we do is very closely follow, when one of these individuals is identified, to find out what he is doing; for instance, at the present time, I am furnishing a list to the offices which did work in this latest round to see if through the work papers that they recover through search and seizure, or through any of the interviews of the subjects, they have any evidence that they were getting into a Federal Government system. For that I will supply each field office with a list of the identities of the various systems so that even if the person does not cooperate they should be able to look through the list of work notes and find if they have any of these systems which appear to be targets for access.

Mr. GLICKMAN. Well, I—this is probably not your responsibility to initiate, but I go back to my point with Mr. Wright of the Office of Management and Budget, it would seem to me that besides Government systems, we have 8 or 10 systems in this country—banking, communications, telephone, power, electric generating, and all that—that relate to the public by reason of the computer as well as through communications systems. And there needs to be some focus from the Government's point of view how we are going to protect those systems. And I think we have done probably a pretty good job of protecting your system and the Department of Defense. But I am not sure that we have done a great job of protecting the systems that affect the daily lives of human beings out there. And that is not—I mean, you are—from an investigative point of view, that's not your role. But I think your comments are useful.

Let me just summarize—ask you to summarize again. You are not here to recommend specific legislation to us, I don't think. But if—if you would advise me on what additional tools you need from a legislative point of view to help deal with some of those problems, what would they be?

Mr. CLARKE. I think in the area of describing the computer property itself so that it adequately describes not only the tangible but the intangible, that it described what is meant by damage and that there be language that deals with the issue of trespass, unauthorized access to that data base.

Mr. GLICKMAN. So you would say nature of the crime, nature of damage, and should the—should the concept of trespass be included, let's say in Federal law with or without any other proof of destruction or theft or larceny, or anything else.

And I don't—you are saying these subjects are not really currently covered under existing statutes, then?

Mr. CLARKE. That is—that is correct. And also, that in dealing with some statutes as to which institutions might—might be covered by the particular legislation.

Mr. GLICKMAN. And would you say that as the issue grows that your—your ability to protect citizens from crime would be impaired if Congress or State legislative bodies didn't move on some of these subjects?

Mr. CLARKE. I am not in a position to make a definitive statement in response to that. I—one other thing that I would like to add, too, is that I think it would be helpful that if attendant to that legislation would be a requirement for institutions who would be covered to report any trespass or attempted trespass, or damage, or unauthorized acess that would be covered by the particular statute.

I think that that would be helpful.

Mr. GLICKMAN. OK. We thank you all for excellent testimony today. Appreciate it.

Our last witness today is Richard Shriver, Assistant Secretary of the Treasury for Electronic Systems and Information Technology.

Mr. Shriver, it is a pleasure to have you today. We are most appreciative. You might want to identify the people who are with you today and then you may feel free to summarize your statement if you wish.

STATEMENT OF RICHARD H. SHRIVER, ASSISTANT SECRETARY OF THE TREASURY, ELECTRONIC SYSTEMS AND INFORMATION TECHNOLOGY, ACCOMPANIED BY DR. BOB CONLEY, DEPUTY, ADVANCED TECHNOLOGY; JOE BISHOP, DEPUTY, PROGRAMS AND RESOURCES MANAGEMENT, AND PAUL TRAUSE, INSPECTOR GENERAL, U.S. TREASURY

Mr. SHRIVER. Yes, sir. Thank you, Mr. Chairman.

I would like to introduce the Treasury people here: Paul Trause, on my left, who is Inspector General. And then two members of our group: Dr. Bob Conley, Deputy Assistant Director of Advanced Technology, and Joe Bishop, Deputy Assistant Secretary for Programs and Resources.

Mr. GLICKMAN. Fine.

Mr. SHRIVER. I thought that it would be appropriate to submit our written statement for—for the record. And given the testimonies that you have had, I would like to try and summarize those points that I feel are—are relevant to Treasury, and not read the testimony itself.

First of all, this is an enormously complex area as it certainly has been clear here this morning. And I think Mr. Regan, in forming our office earlier this year, formed it in part in response to the tremendous need within Treasury, just one of the civil agencies, to have someone and a staff group that was concerned with, amongst other things, the security of information systems.

The media with which Treasury is concerned include radios, and we have heard a great deal about that from the FBI, and we have many of the same problems, particularly in law enforcement and the protection of high ranking Government officials, domestic and foreign.

The telephone system, of course, is a major media, and message systems in the form of teletypes, and so on. This is especially critical with regard to financial information and market data. And naturally we have many computers in Treasury, some 200 major computer systems, that store various kinds of information which I will mention briefly.

We do have, of course, information that relates to law enforcement operations in four Treasury bureaus. We do have conversations that go across the media on various topics, and we do have messages that go across these media on various topics.

We do have data on U.S. citizens in the Internal Revenue Service, amongst others, and we do have economic information relating to markets and the stability of those markets as well.

We also are amongst the largest transmitters of financial information via electronic funds transfer. We currently transfer about a quarter of Treasury's payments electronically—200 million payments per year, or collections per year. And those electronic funds transfers amount to some $200 billion.

And, of course, we also have classified information in the national security sense. So we have a wide variety of problems requiring improved security and attention to security.

The information that we have to protect is of interest to various categories of people who are not authorized to have that information. They range from foreign agents to criminals to—you mentioned the word hackers. I think when there is damage of some sort they certainly are, in our view, vandals, at best.

Now we have several programs to assess and to take action, corrective action, to fix the systems of Treasury. There are both technical and management problems, and I would simply list these and we can discuss these in more detail if you desire.

In April or May—April, March of this year, we formed a Treasury Systems Review Committee, and I think this is very important and very much on target with some of the topics discussed here this morning.

This—this committee is made up of the senior line managers of Treasury and is chaired by the Deputy Assistant Secretary—the Deputy Secretary of the Treasury, Mr. McNamar, and all items relating to the progress of systems, the security of systems, the expenditures and the plans, and so on, are reviewed at a very high level—Treasury management group.

Last week, for example, at a meeting of this group, we approved temporarily, because it is still out for coordination, a new policy on risk management that will apply to all Treasury systems and the substance of that is that it puts the senior line managers again, in other words, the bureau heads, directly responsible for the security of the systems in their area.

That is different than saying that the senior systems or the senior technical person is responsible for the protection of those systems.

We also have worked extensively with NSA, with the National Bureau of Standards, we are currently working with them, and with OMB, to acquaint them with their problems to elicit their support from either a technical standpoint or from a financial standpoint.

We have had two meetings, joint government and industry meetings, those meetings have been very helpful to us in understanding how far private industry has progressed, how we might assist one another. I would add that they are informal discussions simply to assess a base line of where we collectively stand and how we can help each other.

With regard to radio communications, which is a major problem within Treasury, we have had and do work jointly with many enforcement agencies and other Federal agencies that have an interest in this.

At our most recent such meeting, we did have—include the FCC, the FAA, Coast Guard, the National Security Adminis—Agency—DEA, FBI, Customs; Alcohol, Tobacco and Firearms, Internal Revenue Service, and the U.S. Secret Service.

The—we have also heightened the awareness of the importance of security throughout Treasury by a variety of means, including having people meet with the senior managers of Treasury to—from FBI or NSA—and acquaint them with the threat to our communications.

We certainly applaud your efforts to aid the civil side of Government as a part of your effort here and would be pleased to answer any questions you might have.

[The opening statement of Mr. Shriver follows:]

OPENING STATEMENT
RICHARD H. SHRIVER
ASSISTANT SECRETARY OF THE TREASURY
(ELECTRONIC SYSTEMS AND INFORMATION TECHNOLOGY)
BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
HOUSE COMMITTEE ON SCIENCE AND TECHNOLOGY

OCTOBER 17, 1983

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE:

I AM PLEASED TO BE WITH YOU TODAY TO DISCUSS SECURITY THREATS TO, AND VULNERABILITIES OF, COMPUTER AND TELECOMMUNICATIONS SYSTEMS. IN MY TESTIMONY, I WILL DISCUSS MY PERCEPTION OF THE PROBLEM AND THE POSITIVE STEPS TREASURY IS TAKING TO UNCOVER THREATS TO OUR SYSTEMS AND IMPLEMENT SOLUTIONS TO NEUTRALIZE THESE THREATS.

WITH ME TODAY ARE DR. BOB CONLEY, MY DEPUTY FOR ADVANCED TECHNOLOGY AND JOE BISHOP, MY DEPUTY FOR PROGRAMS AND RESOURCES MANAGEMENT. ALSO WITH ME IS PAUL TRAUSE, TREASURY'S INSPECTOR GENERAL. WE WILL BE AVAILABLE TO ANSWER ANY QUESTIONS YOU OR THE MEMBERS MAY HAVE AT THE CONCLUSION OF MY TESTIMONY.

TREASURY'S ASSESSMENT OF THE PROBLEM

THAT TREASURY IS SERIOUSLY WORKING ON THE SAME PROBLEMS YOU

ARE EXPLORING IN THIS HEARING IS DEMONSTRATED BY THE FACT THAT I HAVE BEEN INVITED AS A WITNESS. NO OTHER DEPARTMENT OUTSIDE OF DEFENSE HAS ESTABLISHED AN ASSISTANT SECRETARY-LEVEL POSITION CHARGED SOLELY WITH IMPROVING THE EFFICIENCY, EFFECTIVENESS AND SECURITY OF ITS VITAL COMPUTER AND TELECOMMUNICATIONS SYSTEMS. THE EMPHASIS TREASURY IS NOW PLACING ON SYSTEMS SECURITY IS DIRECTLY ATTRIBUTABLE TO SECRETARY REGAN'S FORESIGHT. UPON TAKING OFFICE, SECRETARY REGAN PERCEIVED THAT TREASURY FUNDS WOULD BE INCREASINGLY TRANSFERRED BY ELECTRONIC MEANS AND THAT MODERN, SECURE SYSTEMS WERE NEEDED. WITH TREASURY NOW HANDLING OVER 800 MILLION FINANCIAL TRANSACTIONS YEARLY, ISSUING OVER 600 MILLION CHECKS AND MAINTAINING ACCOUNTS FOR OVER 100 MILLION TAXPAYERS, THE SECRETARY'S EMPHASIS ON SYSTEM SECURITY AND MODERNIZATION IS WELL PLACED.

UPON MY ARRIVAL AT TREASURY, I COMMISSIONED A PRELIMINARY SURVEY TO DOCUMENT THE EXISTING INVENTORY OF COMPUTER AND TELECOMMUNICATIONS SYSTEMS. INCLUDING THE LARGE SYSTEMS MAINTAINED BY IRS FOR TAX ADMINISTRATION PURPOSES, TREASURY HAS NEARLY 200 AUTOMATED SYSTEMS IN OPERATION TODAY. WE BELIEVE TREASURY IS THE SECOND LARGEST MANAGER OF AUTOMATED SUPPORT SYSTEMS IN THE FEDERAL GOVERNMENT.

IN LOOKING AT THE DATA CONTAINED IN THESE SYSTEMS, WE DETERMINED THE FOLLOWING TYPES OF POTENTIAL THREATS TO TREASURY COMPUTER SYSTEMS:

1. THOSE ATTEMPTING TO IMPROPERLY DIVERT GOVERNMENT FUNDS.

2. THOSE ATTEMPTING TO GAIN IMPROPER ACCESS TO SENSITIVE FINANCIAL INFORMATION;

3. THOSE ATTEMPTING TO GAIN IMPROPER ACCESS TO NATIONAL SECURITY INFORMATION.

4. THOSE ATTEMPTING PENETRATION FOR "RECREATIONAL" PURPOSES. THESE ARE THE "HACKERS" RECENTLY COVERED BY THE MEDIA.

5. THOSE ATTEMPTING TO ACCESS TREASURY VOICE (ESPECIALLY RADIO) COMMUNICATIONS SYSTEMS TO AVOID DETECTION OR APPREHENSION BY TREASURY ENFORCEMENT BUREAUS.

MY OFFICE HAS WORKED VERY CLOSELY WITH THE TREASURY INSPECTOR GENERAL, PAUL TRAUSE, AND WITH HIS STAFF TO ANALYZE THE RESULTS OF OUR INITIAL SURVEY OF TREASURY COMPUTER AND

TELECOMMUNICATIONS SYSTEMS AND, TO ASSESS THE THREAT POTENTIAL OF THE FIVE CATEGORIES JUST ENUMERATED. FROM A SECURITY PERSPECTIVE, TREASURY'S INVENTORY OF AUTOMATED SUPPORT SYSTEMS REPRESENTS A TWO-EDGED SWORD. ON THE ONE HAND THE DEGREE OF CENTRALIZATION IN OUR CURRENT AUTOMATED SYSTEMS MEANS THAT FEWER INDIVIDUALS NOW HAVE ACCESS THAN WOULD BE THE CASE IF MANUAL PROCESSING WERE RELIED UPON. FROM A SECURITY STANDPOINT THIS IS GOOD. AMONG THOSE WITH ACTUAL PHYSICAL ACCESS, FEWER STILL HAVE SUFFICIENT TECHNICAL EXPERTISE TO "BEAT" AUTOMATED SYSTEM SECURITY PRECAUTIONS. ON THE OTHER HAND, IF SOMEONE IS ABLE TO OVERCOME AUTOMATED SYSTEM SECURITY SAFEGUARDS, THE POTENTIAL OF THEIR "BEATING" SYSTEMS IN A BIG WAY IS MUCH HIGHER.

PERHAPS AT TREASURY WE HAVE BEEN FORTUNATE. WE HAVE NOT UNCOVERED ANY BREACHES OF SYSTEM SECURITY THAT COULD BE CLASSIFIED AS A PENETRATION. HOWEVER, WE DO OCCASIONALLY UNCOVER IMPROPER USE OF TREASURY SYSTEMS BY OUR OWN EMPLOYEES. SUCH INSTANCES TEND TO BE INFREQUENT AND ARE DEALT WITH IN SUMMARY FASHION, INCLUDING DISMISSAL AND PROSECUTION. TO DATE, WE HAVE NOT DISCOVERED PENETRATIONS BY OUTSIDERS THROUGH DIAL-UP OR ANY OTHER IMPROPER MEANS OF ACCESS. MONITORING OF OUR TELECOMMUNICATIONS, TELEPHONE, DATA, AND RADIO, IS A SERIOUS AND IMMEDIATE CONCERN, HOWEVER.

TREASURY'S SYSTEMS SECURITY PROGRAM

THE LACK OF KNOWN PENETRATIONS HAS NOT DIMINISHED IN ANY WAY THE IMPORTANCE WE ATTACH TO SYSTEM SECURITY, HOWEVER. WHILE THERE MAY BE LESS HERE THAN MEETS THE EYE AT PRESENT, WE CONTINUE TO TREAT ALL FIVE CATEGORIES OF POTENTIAL THREATS TO TREASURY SYSTEMS AS BEING VERY REAL. WITH SECRETARY REGAN'S STRONG SUPPORT, MY OFFICE, THE INSPECTOR GENERAL'S OFFICE, AND STAFF OF THE ASSISTANT SECRETARY (ADMINISTRATION) ARE JOINTLY IMPLEMENTING A THREE POINT PROGRAM TO ENSURE THE CONTINUED SECURITY OF TREASURY TELECOMMUNICATIONS AND COMPUTER SYSTEMS. THIS PROGRAM INVOLVES:

1. INCREASING SECURITY AWARENESS THROUGHOUT THE DEPARTMENT;

2. DESIGNING AND INSTALLING EFFECTIVE SECURITY MECHANISMS INTO BOTH NEW AND EXISTING SYSTEMS; AND,

3. MONITORING ADHERENCE TO PROPER SYSTEMS SECURITY PROCEDURES.

I WILL NOW DISCUSS SOME THINGS WE HAVE ACCOMPLISHED AND PLAN FOR THE FUTURE TO FURTHER TREASURY'S SYSTEMS SECURITY PROGRAM.

1. IMPROVED SECURITY AWARENESS. FIRST, WE FEEL THAT INCREASING SECURITY AWARENESS IN USING AND MANAGING AUTOMATED SUPPORT SYSTEMS MUST START AT THE TOP. IN TREASURY, WE HAVE NOT ONLY HAD THE SECRETARY'S COMPLETE SUPPORT, BUT THE DEPUTY SECRETARY ALSO IS DIRECTLY INVOLVED IN MANAGING THE DEPARTMENT'S SYSTEM SUPPORT ASSETS. DEPUTY SECRETARY MCNAMAR CHAIRS THE TREASURY SYSTEMS REVIEW COMMITTEE, WHOSE MEMBERSHIP IS MADE UP OF EXECUTIVES DRAWN FROM THE HIGHEST MANAGEMENT LEVELS OF THE DEPARTMENT.

THIS COMMITTEE MEETS BI-MONTHLY. MEETINGS GENERALLY LAST HALF A DAY, DURING WHICH TIME THREE TO FIVE SYSTEMS ARE REVIEWED. SECURITY CONCERNS ARE ROUTINELY DISCUSSED WHEN REVIEWING INDIVIDUAL SYSTEMS. THE SYSTEMS REVIEW COMMITTEE REVIEWS THE RESULTS OF AUDITS CONDUCTED BY THE TREASURY INSPECTOR GENERAL, WHO ATTENDS THESE MEETINGS AS AN OBSERVER. FINALLY, ALL POLICY DIRECTIVES DEALING WITH COMPUTER AND TELECOMMUNICATIONS SYSTEMS, INCLUDING THOSE DEALING WITH SYSTEMS SECURITY, ARE REVIEWED BY THE COMMITTEE. IN SHORT, WE ARE MAKING SYSTEMS PROTECTION AT TREASURY A RESPONSIBILITY OF SENIOR-LEVEL LINE MANAGERS.

IN ADDITION, MY OFFICE IS CHARGED WITH DEVELOPING STANDARDS AND DIRECTIVES TO ENSURE PROPER MANAGEMENT AND UTILIZATION OF SYSTEMS SUPPORT RESOURCES. WE HAVE CLEARED AND ISSUED SEVERAL ALREADY. THE MOST IMPORTANT DIRECTIVE DEALING WITH SECURITY CONCERNS IS OUR DRAFT INFORMATION SYSTEMS RISK MANAGEMENT DIRECTIVE. WHILE THIS COMPREHENSIVE DOCUMENT IS STILL IN THE REVIEW PROCESS, IT SHOULD BE ISSUED SOON AND WILL PROVIDE A FIRM FOUNDATION FOR PROPERLY MANAGING SYSTEMS SECURITY THROUGHOUT THE DEPARTMENT. THE DRAFT DIRECTIVE INCLUDES SUCH TOPICS AS HOW TO ESTABLISH A RISK MANAGEMENT PLAN; CRITERIA FOR REVIEWING AND AUDITING SUCH A PLAN; GUIDELINES FOR MAINTAINING PHYSICAL, TECHNICAL AND PERSONNEL SECURITY; AND A DISCUSSION OF COMPUTER FRAUD AND ABUSE TECHNIQUES. I WOULD BE PLEASED TO FURNISH A COPY OF THIS DRAFT DIRECTIVE TO THE SUBCOMMITTEE IF THE CHAIRMAN SO DESIRES.

ALSO, FROM TIME TO TIME, WE HAVE INVITED THE FBI AND THE NATIONAL SECURITY AGENCY TO PROVIDE THREAT BRIEFINGS TO SENIOR TREASURY PERSONNEL -- BRIEFINGS THAT INCLUDE AMONG OTHER THINGS, THREATS TO OUR TELECOMMUNICATIONS AND OTHER SYSTEMS.

AT TREASURY, WE REALIZE THAT WE ALSO NEED TO STAY ON TOP OF

EMERGING TECHNOLOGIES AND SYSTEM SECURITY DEVELOPMENTS IN THE PRIVATE SECTOR. BANKING AND INSURANCE ARE TWO IMPORTANT INDUSTRIES IN THIS REGARD. WE HAVE ARRANGED TWO INDUSTRY/GOVERNMENT WORKSHOPS TO ASSESS THE FUTURE SCOPE AND MAGNITUDE OF ELECTRONIC FUNDS TRANSFERS (EFT'S).

BOTH OF THE WORKSHOPS HELD THUS FAR WERE WELL ATTENDED BY OTHER FEDERAL AGENCIES AND PROVED TO BE A VALUABLE SOURCE OF INSIGHT. WE FORESEE HOLDING MORE OF THESE FORUMS. TELECOMMUNICATIONS SECURITY WILL LIKELY BE A SUBJECT OF ONE OF OUR UPCOMING INDUSTRY/GOVERNMENT WORKSHOPS.

2. DESIGN AND INSTALLATION OF SECURITY MECHANISMS. AT TREASURY, FOUR COMPLEMENTARY MECHANISMS SERVE TO ENSURE THAT THE OVERALL DIRECTION SET AT SYSTEMS REVIEW COMMITTEE MEETINGS IS CARRIED OUT. THESE MECHANISMS ARE: APPROVAL BY MY OFFICE OF ALL SYSTEMS PROCUREMENTS ABOVE $250,000; MANAGEMENT OF THE TREASURY TELECOMMUNICATIONS STEERING GROUP BY MY OFFICE; MY STAFF'S INVOLVEMENT WITH THE BUREAUS ON SECURITY ASPECTS OF INDIVIDUAL PROJECTS; AND, THE INSPECTOR GENERAL'S INVOLVEMENT IN SYSTEM REDESIGN EFFORTS. AUDITORS FROM THE INSPECTOR GENERAL'S STAFF REVIEW THE SYSTEMS DESIGN PROCESS TO: ENSURE THAT SUFFICIENT INFORMATION IS DEVELOPED FOR MANAGEMENT TO MAKE CRITICAL DECISIONS; PROVIDE TECHNICAL ASSISTANCE IN DEVELOPING PROPER

INTERNAL CONTROL; AND, TO ENSURE THAT APPROPRIATE AUDIT TRAILS ARE ESTABLISHED.

BEFORE ACCEPTING MY CURRENT POSITION, I WANTED TO ENSURE THAT MY OFFICE WOULD HAVE SUFFICIENT AUTHORITY TO GET THINGS ACCOMPLISHED AT ALL LEVELS IN THE DEPARTMENT. NOT FORGETTING THE WAYS AND WILES OF WASHINGTON FROM MY PRIOR GOVERNMENT SERVICE AS AN ASSISTANT SECRETARY OF DEFENSE DURING THE FORD ADMINISTRATION, I HAD A STRONG BUDGET ROLE CLEARLY LAID OUT IN THE MISSION STATEMENT FOR MY CURRENT POSITION. JOE BISHOP, OUR DEPUTY FOR PROGRAMS AND RESOURCES MANAGEMENT, REVIEWS ALL BUREAU SYSTEMS BUDGET PLANS BEFORE THEY ARE SUBMITTED TO OMB, AND AS PREVIOUSLY MENTIONED, REVIEWS PROPOSED SYSTEMS PROCUREMENTS IN EXCESS OF $250,000. IN ANALYZING BUREAU COMPUTER AND TELECOMMUNICATIONS SYSTEMS PLANS, WE KEEP THE NEED FOR PROPER SYSTEMS SECURITY IN CLEAR FOCUS.

MY STAFF ALSO INTERACTS WITH THE BUREAUS AT MIDDLE MANAGEMENT LEVELS TO ENSURE THAT SYSTEMS POLICY DECISIONS ARE IMPLEMENTED PROPERLY. DR. BOB CONLEY, OUR DEPUTY FOR ADVANCED TECHNOLOGY, CHAIRS THE DEPARTMENT'S TELECOMMUNICATIONS STEERING GROUP. THIS GROUP STAYS ON TOP OF TECHNOLOGICAL DEVELOPMENTS IN

THE MARKETPLACE AND IDENTIFIES BUREAU TELECOMMUNICATIONS REQUIREMENTS THAT WILL BE IMPACTED BY THESE DEVELOPMENTS. DR. CONLEY'S STAFF IS ALSO DEEPLY INVOLVED IN SEVERAL KEY PROJECTS, INCLUDING: VOICE PRIVACY TACTICAL COMMUNICATIONS SYSTEMS FOR OUR TREASURY ENFORCEMENT BUREAUS; A PROPOSAL FOR A LARGE, NATIONWIDE TELECOMMUNICATIONS NET TO SERVICE ALL TREASURY BUREAUS AT A REDUCED OVERALL COST; AND A MEANS OF PROVIDING AUTHENTICATOR SYSTEMS TO ALLOW SIMPLER, YET MORE SECURE SYSTEMS ACCESS FOR TREASURY PERSONNEL OPERATING IN THE FIELD.

BILL CROWELL, OUR DEPUTY FOR FINANCIAL SYSTEMS, HAS HEADED UP OUR WORK IN THE AREA OF CASH MANAGEMENT SYSTEMS. BILL'S STAFF HAS HELPED APPLY THE TREASURY FINANCIAL COMMUNICATIONS SYSTEM AND VARIOUS OTHER SYSTEM APPROACHES TO IMPROVING THE DEPARTMENT'S CASH MANAGEMENT PRACTICES. WE HAVE GIVEN SPECIAL ATTENTION TO INCORPORATING PROPER SECURITY MEASURES IN ALL OUR NEW CASH MANAGEMENT SYSTEMS.

3. MONITORING ADHERENCE TO PROPER SECURITY PROCEDURES. MY STAFF AND THE INSPECTOR GENERAL'S STAFF EACH HAVE A ROLE TO PLAY IN MAKING SURE THAT PROPER SECURITY PROCEDURES ARE CARRIED OUT.

THE INSPECTOR GENERAL IS NOW HIRING A TEAM OF DATA PROCESSING SYSTEMS AUDITORS WHO ARE DEVELOPING, AND WILL CARRY OUT, A COMPREHENSIVE AUDIT PLAN FOR ALL THE DEPARTMENT'S MAJOR SYSTEMS. MY STAFF ALSO CONDUCTS BUREAU SYSTEM REVIEWS, WHICH STRESS APPROPRIATE USE OF TECHNOLOGY AND CONFORMANCE WITH POLICY DIRECTIVES ESTABLISHED BY MY OFFICE. WE ARE ALSO WORKING WITH PAUL TRAUSE'S STAFF TO JOINTLY PROMOTE THE CONCEPT OF BUILDING MAJOR NEW SYSTEMS WITH INTEGRATED TEST FACILITIES, A PROCEDURE THAT WILL ALLOW QUICKER, MORE COMPREHENSIVE SYSTEM AUDITS IN THE FUTURE. FINALLY, TREASURY MONITORS SYSTEM SECURITY BY USING INNOVATIVE COMPUTER MATCHING TECHNIQUES. FOR EXAMPLE, TREASURY RECENTLY MATCHED REVENUE SHARING DISBURSEMENTS AGAINST A FILE OF ELIGIBLE STATE AND LOCAL GOVERNMENTS TO IDENTIFY POSSIBLE QUESTIONABLE PAYMENTS. IN THIS PARTICULAR EXERCISE, NONE WERE FOUND.

NEED FOR ADDITIONAL MEASURES

AT TREASURY, WE HOPE THAT OUR THREE POINT SYSTEMS SECURITY PLAN WILL ENABLE THE DEPARTMENT TO STAY AHEAD OF CURRENT THREATS AND POSITION US TO NEUTRALIZE FUTURE THREATS. ALL GOVERNMENT

SYSTEMS MANAGERS MUST ALSO KEEP UP TO DATE WITH TECHNOLOGY TRENDS THAT WILL IMPACT ON SECURITY THREATS. MAINTAINING EFFECTIVE LIAISON WITH OUR PRIVATE SECTOR COUNTERPARTS IS ONE APPROACH WE HAVE USED AT TREASURY. WE ALSO TRY TO KEEP CHANNELS OF COMMUNICATION OPEN WITH THE VENDOR COMMUNITY.

I DO NOT FEEL THE COMPUTER AND TELECOMMUNICATIONS SECURITY PROBLEM IS PRIMARILY ONE OF INADEQUATE LAWS. WHAT DOES DISTURB ME ARE THE TRENDS WE HAVE OBSERVED IN THE SENTENCING OF THOSE CONVICTED OF COMPUTER FRAUD. SOME STATISTICS I RECENTLY RAN ACROSS INDICATE THAT AN AVERAGE BANK ROBBERY NETS AROUND $20,000. IF CAUGHT, BANK ROBBERS ARE PROSECUTED AROUND 90% OF THE TIME AND, IF CONVICTED, WILL ON THE AVERAGE BE SENTENCED TO 4-6 YEARS IN PRISON. THE AVERAGE CRIME INVOLVING ELECTRONIC FUNDS TRANSFER IS SOMEWHERE AROUND $500,000. IF CAUGHT, PERPETRATORS OF SUCH THIEVERY ARE PROSECUTED ONLY 15-20% OF THE TIME AND, IF CONVICTED, CAN EXPECT TO SPEND ONLY 4-6 MONTHS IN PRISON. GIVEN THIS DISPARITY, I QUESTION THE EXTENT TO WHICH OUR JUDICIAL SYSTEM IS HELPING TO DETER COMPUTER CRIME.

LAW ENFORCEMENT SECURITY NEEDS

A MAJOR PROJECT MY OFFICE IS CURRENTLY INVOLVED WITH IS HELPING OUR TREASURY LAW ENFORCEMENT FUNCTIONS (SECRET SERVICE; ALCOHOL, TOBACCO AND FIREARMS; CUSTOMS; IRS CRIMINAL INVESTIGATION; AND, IRS INSPECTION) ACQUIRE SECURE MEANS OF COMMUNICATION. CURRENTLY, TACTICAL LAW ENFORCEMENT OPERATIONS HAVE TO RELY ON OUTDATED RADIO GEAR THAT DOES NOT INCORPORATE NEEDED PRIVACY FEATURES. IT IS NOT ONLY FRUSTRATING BUT IS INDEED DANGEROUS TO SEND OUR LAW ENFORCEMENT AGENTS OUT INTO THE FIELD WITH COMMUNICATIONS EQUIPMENT THAT CAN BE MONITORED BY VIOLATORS USING NOTHING MORE SOPHISTICATED THAN OFF-THE-SHELF SCANNERS. WITH TREASURY NOW WORKING CLOSELY WITH MANY OTHER GOVERNMENT AGENCIES TO CONTROL DRUG SMUGGLING, WE HAVE EVEN MORE NEED FOR SECURE MEANS OF TACTICAL ENFORCEMENT COMMUNICATION. DR. CONLEY IS WORKING CLOSELY WITH ALL THE TREASURY ENFORCEMENT BUREAUS AND WITH THE ENTIRE FEDERAL LAW ENFORCEMENT COMMUNITY TO DEFINE PRIVACY AND SECURE COMMUNICATIONS STANDARDS AND, IF POSSIBLE, TO ARRANGE FOR COORDINATED PROCUREMENTS TO SAVE THE GOVERNMENT MONEY. OUR PLANS AT THIS TIME ARE TO START PROCURING NEEDED EQUIPMENT FOR TREASURY IN FISCAL YEAR 1985. WE ARE ALSO STARTING TO INSTALL SECURE TELEPHONE EQUIPMENT FOR TOP TREASURY POLICY OFFICIALS AND FOR CERTAIN LAW ENFORCEMENT PURPOSES.

MEETING SECURITY NEEDS THROUGHOUT GOVERNMENT

AS YOU MIGHT EXPECT, I FEEL STRONGLY THAT COMPUTER AND TELECOMMUNICATIONS SECURITY AWARENESS NEEDS STRENGTHENING THROUGHOUT GOVERNMENT. WHILE EVERY DEPARTMENT IN THE FEDERAL GOVERNMENT MAY NOT NEED AN ASSISTANT SECRETARY-LEVEL POSITION, EVERY GOVERNMENT AGENCY EMPLOYING COMPUTER AND TELECOMMUNICATIONS SYSTEMS DOES NEED STRONG EMPHASIS FROM THE TOP ON IMPROVING SYSTEMS SECURITY.

CONCLUSION

MR. CHAIRMAN, I HAVE ATTEMPTED TO COVER IN MY BRIEF STATEMENT SOME OF THE THINGS WE ARE TRYING TO DO AT TREASURY TO KEEP AHEAD OF THE SYSTEMS SECURITY PROBLEM. WE RECOGNIZE THAT WE DON'T HAVE ALL THE ANSWERS AND THAT NO MATTER HOW MUCH WE HARDEN OUR SYSTEMS, WE WILL NEVER BE ABLE TO DEVELOP TOTALLY IMPENETRABLE SYSTEMS. OUR STRATEGY IS TO MAINTAIN A COMPREHENSIVE PROGRAM THAT NOT ONLY FOCUSES ON TECHNOLOGICAL SOLUTIONS, BUT ALSO STRESSES PEOPLE SOLUTIONS. MY OFFICE WOULD CERTAINLY BE PLEASED TO SHARE OUR SECURITY KNOWLEDGE AND EXPERIENCE WITH OTHER FEDERAL GOVERNMENT AGENCIES.

MY ASSOCIATES AND I WILL BE PLEASED TO ANSWER ANY QUESTIONS YOU OR THE MEMBERS MAY HAVE.

Mr. GLICKMAN. Thank you very much.

In summary, then, you do not—at least indicate—to date you do not feel there's been a serious problem of illegally entering any of the computer systems that you have jurisdiction for, and your Inspector General is here. I am just curious if there have been any cases yet in which——

Mr. SHRIVER. Let me give you a broad comment and then I would like to ask Mr. Trause to comment specifically. The answer is that there—yes, there—we have—we have not had serious penetrations of computer facilities. At the moment we believe there is really less there than meets the eye but the vulnerability is there and it is growing, and that is—that is the reason why we are so concerned.

I don't want to end it at that because we have very real and current problems in other areas that do not involve computers, such as radio and telephone.

Mr. GLICKMAN. OK.

Mr. SHRIVER. Do you want to add to that?

Mr. TRAUSE. I think that that is very much true. I think there has been a failure to recognize—excuse me—that at the same time that the computer has heightened the risk, heightened the stakes, it has also made it much easy—much easier for us to control transactions, particularly where you are dealing with large volume, small dollar transactions, because it cuts down the amount of human handling.

As of today, we have not had a major problem. That does not mean that we won't, that does not mean that the potential is not there—it is.

Mr. GLICKMAN. Tell me basically the kinds of systems that you have with respect to sub—subject areas, substantive areas—some of your bigger systems. I mean, you know, I am trying to figure out, are they dealing with Treasury bills, or we are dealing—you know, how, how—relate this to me as a lay person.

Mr. SHRIVER. Actually, Treasury bills are handled through our fiscal agent, the Federal Reserve; and we, in fact, have very little. We do keep track of a small portion of that but predominantly public debt is handled through computer systems of the Federal Reserve, and increasingly so in the future.

But the areas that are of greatest concern relate to taxpayer information, and virtually every taxpayer, and then some, in the country. Also, enforcement information. There is a—there are substantial data bases, about 50, that deal with the enforcement problem throughout the four Treasury bureaus that have an enforcement role. And these are very extensive, ranging from lookout systems to identified persons crossing our borders, to supporting the DEA, and drug interdiction efforts, to, of course, the Secret Service, and protection against various kinds of people who may not, in fact, be criminals at this point.

But in addition, we have, as I mentioned, the tremendous cash disbursements and collection effort of Treasury, and those are very important systems to us, and ones where we pay a lot of attention.

Mr. GLICKMAN. Now, you talk about the increased vulnerabilities. Let's go through these. Where are the increased vulnerabilities? Let's first look at the income tax system, the—I wonder if you might want to share where the vulnerabilities are in each one of the systems you mentioned, potential vulnerabilities.

Mr. **Shriver**. Well, I would like to ask Mr. Bishop, who came to us from the Internal Revenue Service, and was the senior systems person in the IRS, to answer your first question.

Mr. **Glickman**. Sure.

Mr. **Bishop**. As the data base increases in the use of the mini and microcomputers increases, the vulnerability would increase also.

Mr. **Glickman**. You need to speak up a little bit.

Mr. **Bishop**. More and more there is reliance on the office automation and the microcomputer area, and the data bases are becoming decentralized. And as that happens there is an increase in the access to the base and, therefore, an increase in the vulnerability.

Mr. **Glickman**. Increase to access by whom?

Mr. **Bishop**. By our employees.

Mr. **Glickman**. So you have more and more people who work for the IRS who have increased——

Mr. **Bishop**. Yes, that's right.

Mr. **Glickman** [continuing]. Access?

Mr. **Bishop**. Yes.

Mr. **Glickman**. Has this caused you a problem to date? Have you had any problems with improper access by IRS employees?

Mr. **Bishop**. Yes, there was. There has been problems in the past, both inquiring against accounts they had no business inquiring against. And there have been one or two cases of embezzlement through the use of the system. The embezzlements I know of were prosecuted, and successfully prosecuted.

Mr. **Glickman**. OK.

Mr. **Shriver**. I think it is very important that the IRS sends back to the taxpayers some—I think it's 80 million—payments per year in terms of tax refunds. And, of course, that's—that's just a large number, and it doesn't take a very large percentage to have a significant problem.

Mr. **Glickman**. OK. Now, the IRS is one area. What other areas under your jurisdiction where you might have some increased vulnerabilities as time goes on?

Mr. **Shriver**. Well, the enforcement area is—are we talking specifically about computers or the total area?

Mr. **Glickman**. No; I think the total, because this subcommittee is really concerned about communications generally as well.

Mr. **Shriver**. The one that—that I feel most strongly about personally in terms of fixing it as quickly as we can because the effectiveness of our—our effectiveness is at risk and lives are at risk, and that is in the enforcement area. And we have thousands of enforcement people who work jointly with Coast Guard and DEA. And you heard good testimony from the FBI just a few minutes ago on this very same subject. And I think the people from NSA and Defense Department would tell you how difficult it is for three different parts of the Government to work together in a joint operation and be able to talk to each other with common communications equipment and yet still have the privacy that they need from the media that can expose an operation as well as from the criminal element who, for a few hundred dollars, can sit and listen in—I think it's $15—to get all the Federal law enforcement radio frequencies. So we don't know how much we are missing.

And that's such an important problem to this country that—that I feel personally, and I know a lot of others share this feeling—that that's an area of tremendously high priority to Treasury. And we must work together to solve the national problem with DEA and with the Coast Guard.

Mr. GLICKMAN. Sometimes I notice the media shows up to film the arrest.

Mr. SHRIVER. Well, that's the case in point that I was not going—I will allude to, did involve the death of an Alcohol, Tobacco and Firearms agent. It is not certain that the me—one cannot say that the—that the media, showing up to film the arrest, caused the death, but it certainly alerted the criminal that something was happening. And—and the ATF agent was—was killed.

Mr. GLICKMAN. Let me ask you a little bit—again, I'm going back to institutional problems. The first witness here—I don't know if you were here then or not—was the——

Mr. SHRIVER. I missed that.

Mr. GLICKMAN [continuing]. Gentleman from OMB. And he basically acknowledged that his agency had—if there was any general coordinating role in government on these issues, it was his agency, although he said that it was primarily delegated down to agencies such as your own.

I wonder if you have any feeling about whether you have been in close contact with the Office of Management and Budget in recent years. Are they helpful to you? Or are you pretty much acting on your own to try to protect the—your own agency's problems?

Mr. SHRIVER. Certainly in terms of understanding the problem and being able to recommend how to solve it, we believe that that's 99 percent our problem, at least in terms—a hundred percent our problem in terms of responsibility. And we work much more closely with NSA and the Defense Department and other—other department—other agencies, to help define the problem, and the solution to it, if part of that solution involves funds.

And in the past, security funds have not made it through the total process. And we are very anxious this year to find out exactly where in the process these funds don't make it. And so we certainly are hoping to tell our story to OMB and hope that they will support us from a budgeting standpoint to fix these problems. They are not inexpensive.

Mr. GLICKMAN. In light of that, do you feel that there are major barriers to organizing an appropriate computer communications security policy in this Government and particularly in your agency?

Mr. SHRIVER. No, sir, I don't think there are major barriers, at least not technological. But I do believe that it will require very high level support, perhaps as high—certainly—in Treasury it starts at the Secretary of the Treasury.

Mr. GLICKMAN. And you are telling me today that you have geared up and you have a comprehensive computer security program and approach at Treasury?

Mr. SHRIVER. I wish I could be quite as—as confident as you said, but I think we are definitely well along that path; yes, sir.

Mr. **Glickman**. What factors prompted you to centralize commuter—computer communication security policy responsibility?

Mr. **Shriver**. Well, this was Mr. Regan's own initiative and he came from a commercial past that where this—the business of technology was incredibly important to him. And he came to Treasury and discovered that it was rather diffuse and decentralized. And, in fact, there was no one at a staff meeting to talk to about this problem.

I'm—and in his first 2 years he became convinced that there was a need to do this.

I mention this because I have heard from other people in other agencies that when they do have a discussion, quite often the agency had—asks a question about systems or technology, and there really is no one in the room to deal with the problem at the staff at the high—at that—at that level.

So I do think there is a significant management issue at stake within the Federal Government—throughout the Federal Government—that can be—can be addressed, and should be.

Mr. **Glickman**. A final question. The banking community in this Nation is using computers almost exclusively to deal with protection of deposits and—and you compound that with this incredible complexity of financial deregulation.

I see an impending disaster with respects to bank—respect to banks who are not prepared in terms of their systems to manage them properly.

And, one, I wonder if you would comment on that assumption on my part and; two, how you can help the banking industry if it's your role at all in assisting them in computer security needs?

Mr. **Shriver**. Well, I know there are at least one or two banks represented here today, including one that I used to work for, that—and, and we did go to sleep at night and worry that enormous assets might move away from the bank with the speed of light to some unknown location.

That problem is very, very serious, I believe, in not just to the banks but to, again, to the stability of the—the financial community within this country.

And they are virtually—in many cases they are not equipped to deal with this. You will find banks and credit card companies hiring today top security people from the FBI, from the Defense Department.

And at the bank that I worked with, I hired a major general, and he hired five colonels, and we really put together a pretty good program.

Mr. **Glickman**. You do this to take over other banks? You hired the military staff——

Mr. **Trause**. Yeah, they called it a tiger team.

Mr. **Shriver**. The point is that the skills are very scarce. And when it gets to international communications and transborder data flows, and voice and data and message, and the tremendous complexity just domestically—it is an enormous undertaking for a major bank. And I think you are finding that that they are really taking strong action internally.

The Federal Government can and is helping in various ways. I think the Secret Service and the FBI jointly have jurisdiction over

EFT, electronic funds transfer, crime, in various ways. And—and we are working with the private sector and they are helping us as well.

Mr. GLICKMAN. Well, you know, there's another kind of—I've been involved in the development of the futures markets through my service on the Agriculture Committee, and I see more and more futures trading are going to—occur probably almost exclusively by computers, some of which is going to be based outside the United States. And you could see if you could disrupt raw commodity availability or process—you could wreak havoc on this country. And there are lot of the same parallels with respect to the banking industry.

Mr. SHRIVER. Market disruption is a very significant concern of Treasury as well as the Department of Agriculture.

Mr. GLICKMAN. I think you have—from what you have said here today, that you—Treasury appears to be a good model for Federal agencies in establishing computer security programs.

I don't think that listening to what I heard from the Office of Management and Budget if indeed they are the ones responsible for establishing these patterns around the Government that other agencies have done the job that you have. They probably don't have the immediates—the immediacy to the threats that you have had either.

But I am appreciative that you have come down here and testified today. You have a final?

Mr. SHRIVER. One final point if I may, sir. We have—we did bring a draft copy, and it's not all that big, although it is big—of our risk management policy. As I say, this is being coordinated amongst the Treasury bureaus but it does represent the best that we could bring together from a variety of sources throughout Government and private industry and we would be happy to—to——

Mr. GLICKMAN. You would like us to at least look at it. I don't know if we want to include it all in the record, but if we could look at it that would be much appreciated.

Mr. SHRIVER. That would be fine.

Mr. GLICKMAN. Let me just ask you a final question. Do you think the laws on the books, in terms of the criminal laws, are adequate? I would ask your Inspector General or you to comment on whether we need to modify those laws.

Mr. TRAUSE. I would share the view that was expressed by the gentleman from the FBI earlier, and that is but if the criminal law needs strengthening, it needs strengthening in the areas that he mentioned. One, the definition of software as property; two, a tightening of the definition or an expanding of the definition of you, if you use the verb, of the concept of trespass.

I think that those are essential changes.

Third—and something I know that Dick will address it at more length than I—is sentencing practices as almost more important than the law itself.

Mr. SHRIVER. Yes, sir. I think that we shouldn't think that the law can solve this problem by itself because there are many other reasons why the following happens: Someone that holds up a bank nets on the average, as I understand it, something in the vicinity of $20,000. If they are pros—if they are apprehended, they go to jail with a probability of 90 percent or thereabouts. And they spend 4 to 6 years in prison.

Someone who commits an EFT crime nets on the average $400,000 to $500,000. If they are apprehended the probability of a prison sentence is somewhere between 15 and 20 percent. And if they do go to prison it is 3 to 4 months.

The reason for that is not all due to the absence of adequate legislation. In part, financial institutions are understandably reluctant to take action that would—that would put a vulnerability in the newspapers and in fact they—they affect some of their assets.

Mr. GLICKMAN. OK. Well, we thank you for some excellent testimony. We appreciate your input and we will probably be working with you in the future on a cooperative relationship. Thank you very much.

Mr. SHRIVER. Thank you.

Mr. GLICKMAN. This concludes the hearings today. Our hearing a week from today will be also on the same subject. We will be focusing on the private sector, banks—who else do we have?—credit card companies, and the like, to try to get a feel from them how they are dealing with this issue.

The hearing is adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

MONDAY, OCTOBER 24, 1983

House of Representatives,
Committee on Science and Technology,
Subcommittee on Transportation,
Aviation and Materials,
Washington, D.C.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2318, Rayburn House Office Building, Hon. Dan Glickman (chairman of the subcommittee) presiding.

Mr. Glickman. Why don't we go ahead and begin this morning our third day of hearings that we have.

I just—while it is not terribly usual, I thought it might be, if nothing else, a good gesture for us just to take a moment of silence in reflection of the 160 or so marines who were killed in Lebanon.

[A moment of silence.]

Mr. Glickman. We today are starting our third day of hearings on the issue of computer and communications security and privacy, and today we will wrap up our inquiry into the subject.

Our first hearings, of course, we heard about the subject of hackers and illegal and unlawful invasion or access into computers. The second hearing heard the Government response, and today we will turn our attention to computer security issues in the private sector.

Computers and the communications links that connect them are becoming even more important to society. Both Government and the private sector are amassing vast amounts of personal data on virtually all our citizens. Businesses of all kinds are moving toward automated point-of-sale systems, involving the transfer, by electronic means, of huge sums of money. The Postal Service, along with a host of private carriers, are offering electronic mail services. In each of these applications, the potential for abuse or loss of personal privacy is immense.

In our hearing last week we found that the Government's attention to this threat is fragmented, at best, and suffers from a distinct lack of leadership from the Office of Management and Budget.

Today we look at how this issue relates to the private sector. To help in this task, we have invited representatives from some of the most forward-thinking companies in their respective industries. In hearing from them, we hope to gain a much better understanding of the threats to our computer-dependent society and hopefully of the actions needed from Government and in the private sector.

Mr. McCandless, do you have any statement today?

Mr. McCandless. No, I have no statement at this time.

Mr. Glickman. OK. Thank you.

Well, if there are any statements to put in from yourself or Mr. Carney, then they will be included in the record at this point.

Mr. Glickman. Our first witness today is Dr. Willis H. Ware, information systems, security and privacy, associated with the Rand Corp. in Santa Monica.

Dr. Ware—there you are—it is a pleasure to have you here. I am—I am advised that you are really the expert in this entire area and the committee is privileged to have you here.

I will say to you, as I will say to all of the witnesses here, you may feel free to summarize your statement, if you wish, because all of your statements will be included in the record.

STATEMENT OF WILLIS H. WARE, INFORMATION SYSTEMS, SECURITY, AND PRIVACY, THE RAND CORP.

Mr. Ware. Yes, sir. In fact, I would like to skip over it rather quickly because there are some new things that I would like to submit for your consideration.

As you mentioned, and I say for the record, I am Willis H. Ware of the Rand Corp. The views I express are mine and not those of the corporation, nor of its research sponsor.

My credentials for addressing this issue are chairing the HEW committee, chairing a Defense Science Board committee that looked at computer security in the late seventies, being a member and Vice Chairman of the Privacy Protection Study Commission, and having written and spoken quite widely on the issue.

I do appreciate your invitation to come and speak this morning because it is an important issue not only for the country, but for me professionally. Let me just hit some high points of my testimony by way of summary.

First, the distinction between security and privacy. Privacy has to do with protecting information about people in computer systems and assuring that it is used for authorized purposes. Computer security has to do with the body of technology that assures that protection. A computer security issue is obviously important, whether it is personal information, whether it is defense information, or whether it is corporate proprietary and private information.

I would make, first of all, the observation that computer security is not a static event. It is a very dynamic one, yet it must be looked at in the same way that the military person looks at the classical offense and defense.

As the defenses of computer security safeguards get better, the offenses that get them—against them will become more sophisticated, and that cycle repeat—will repeat again and again and again.

So, I would urge you, as I would urge any organization, not to regard this as a one-time only, end-of-the-road, leave-it-alone issue. It must be looked at repeatedly, and I would hope that the Congress could see fit to examine it every year or so for at least the next 5 and maybe the next 10 or more years. It is that dynamic.

Now, the threats in computer security differ in the Government defense situation versus the industrial/commercial situation. In the defense situation, the threats that are mounted against information systems are the high technology threats that are mounted by the world powers against us. In particular, they involve very sophisticated technological threats. They also involve people threats, as we have all read on many occasions.

In the commercial sector, the people threat is the dominant one at this point in time. If one examines the perpetrations that have occurred and the Parker data base at SRI, he finds that in almost every instance the penetration or the perpetration of crime was by an individual authorized within the system and in some way knew enough about it to exploit it.

At the moment, the technical threats are minimal but when the private sector gets its act together with regard to protecting against people, with regard to protecting against low-level technical threats, at some time in the future, then, the sophisticated technical threat will become more important.

Now, what can we do about all of that? A salient observation that I would make is that technology is not—is not the issue. There's lots of technology around. There are many technological safeguards that could be installed and would be effective. There is also a lot of procedural and administrative safeguards that could be important deterrents.

From my point of view, what must happen in the private sector is the corporate will to address the problem and a corporate commitment to put the issue on a par with the protection of other valuable resources. By implication, of course, we would need a corporate commitment to spend whatever modest sums are needed.

Now, what can we do about simple technical threats? I am sorry, what can we do about the people threats? And that is a hard one because one can't legislate honesty into people. The defense community, of course, makes wide, extensive background investigations to assure trustworthiness of people but even that might not reveal latent or deeply seated problems.

So, first of all we must do what we can with technical and procedural safeguards because a good array of them will fend off some of the people problems. Then we might take legal steps, and I have suggested some in my testimony that I won't repeat here.

But what about technical safeguards? There are attractive options, and I think we should get on with that. For example, when one logs on to a system, normal systems will permit him to make an indefinitely large number of tries, so it is easy for the hacker to guess his way in and as you so adroitly saw portrayed in "War Games" very realistically and very accurately how it is done.

Now, there are opportunities to fend off that kind of threat. Clearly such an arrangement—namely, indefinite number of log ons—is both undesirable and unsafe, and there is no reason why a computer system shouldn't disconnect any individual who is attempting to play that sort of game.

I would point out that it can be done. The Los Alamos National Laboratory has done it, although Mr. Clary's testimony did not happen to mention it.

What it involves is an arrangement in which an individual is disconnected automatically from the system after he makes a certain number—three, four, five—unsuccessful tries. And in the Los Alamos arrangement, the requirement is that the individual take himself in person to the computer security center and explain why he can't type before he gets back on to the system. And if he manages to blow it for another series of tries, then his supervisor is obligated to explain in writing why this individual cannot type.

Now, that is admittedly an annoying arrangement for any person, but on the other hand, that is the kind of safeguard that we can institute technically and that would be effective against some of the game playing and the threats that are going on.

So, we need a menu of such technical features, and I would offer you this recommendation. I would suggest that you task the Institute of Computer Science and Technology in the National Bureau of Standards to produce such a list of options and consider making that list of options mandatory in Government acquisition of computers.

Let's turn now to where the Government will seek wisdom on some of these issues.

On many aspects of computer security are already well in hand because the Department of Defense has worked many of them, personnel security, physical security, TEMPEST security and so forth, so there is no need to go further with that.

Your principal assets in going further you have heard from on the 17th: Computer Security Center at NSA, the ICST at NBS, and the GSA.

Now, CSC, as you know from its testimony, is focused on what is called trusted systems. It is a DOD entity and, therefore, its focus of concern will be on defense systems and, in particular, on sophisticated technical threats. It will not be concerned with the general administrative and procedural environments in which secure systems must be operated.

ICST over at the NBS is also in technical work, as you know, but what the Government needs is a comprehensive, let me call it a handbook, that says here is how one runs the computer center of security; here are the procedural and administrative safeguards that must be in place; here are the risks that people represent; here is what can be done against those risks; here are the general administrative protective measures that can be taken, and on and on.

No one has addressed that issue, there is no comprehensive policy of that kind in place and, therefore, every agency is winging it, every agency is doing it for itself. Some, I gather, are not at all. It is best being done piecemeal. And, of course, in the private sector, each major corporation builds its own policy structure and implementing details.

How do we get that comprehensive guidebook? I would suggest that since the GSA is deeply in the Government acquisition and control of computers, it would be reasonable to ask of it that the GSA compile such a comprehensive handbook of preferred practices and procedures for running a computer center securely. In my view that is not a big undertaking. It is not hundreds of people for tens of years. It is a few people for a year or two.

At some point in time we may have in place at the Federal level a Federal center of some kind. At that juncture, these are appropriate tasks for the center to undertake but for the moment I see no reason why the assets that the Government now holds ought not get on with working the problem.

Now, let me turn from computer security to privacy. First, I would like to clarify a statement which I believe Congressman Wirth made. I disagree strongly with his observation that all the aspects of privacy have been attended.

First, most of the recommendations from the Privacy Protection Study Commission have not been implemented by law but, moreover, there are new dimensions of privacy that have developed since the PPSC and which were not identifed nor treated then.

What we are seeing is the emergence of systems that contain information about people but for other than recordkeeping purposes. And of course, it was privacy in the recordkeeping context that the Privacy Commission examined.

Let me illustrate all of this in the context of electronic mail, which I imagine has been discussed for you already, which the U.S. Postal Service is marketing as ECOM. An electronic mail system, of course, is intended to deliver messages from one individual or one organization to another.

So, in addition to the message content within the system, there will be lots of personal information in terms of addressee-sender pairs, which is a wonderful body of information that could be attractive and of high interest to many outsiders. The legal umbrella for that body of information is spotty. It is incomplete and confused.

I would like to add to what I have submitted to you in writing some further clarification of the electronic mail system because of some information that became available to me just this past week.

In one Federal agency the in-house investigative staff on at least three occasions obtained a complete printout of the electronic mail system that provided office automation support. On at least one of those occasions an outside law enforcement agency was involved.

In effect, several hundred workers who use electronic mail in the conduct of their business had all their computer records read, and in at least one instance an individual was intimidated. The privacy of the workplace records of hundreds of people had been invaded and hundreds of people were caught up in an investigative sweep without any recourse to protect themselves.

It all sounds very much to me like search and seizure without due process of law, or at least it sounds like a fishing expedition, trying to find out if something has gone wrong. In this instance, the computer happened to be Government owned. One can't help but wonder what the situation might have been if the mail service had been provided by a commercial vendor whose computer would have been located on private premises.

I, of course, don't know the motivations of the investigative groups. Perhaps they were tracking down hackers or perhaps there was some possible fraud or embezzlement, but in any event, there is no reason—and I do not wish to make this incident a cause celebre—but it is a useful one to underscore the ease with which new privacy issues arise as computers plus communications are exploited to provide a wide variety of new services to a wider and wider population of users. This is an example of a new dimension of privacy, and I have labeled it "access without action."

Computer matching files exhibits exactly the same dimension. Individuals who happen to keep records in the computer system or individuals who are record subjects in some file have their privacy invaded whether or not an individual has done something wrong. Private information gets exposed to a third party and possibly exposed to hostile eyes.

In effect, in the example I cited, all the hundreds of office workers or all the data subjects in a computer file were a priori assumed to have been guilty. The examination or the matching of computer records then proceeded in an effort to demonstrate that they were not, which all sounds very much like back end to justice.

I label this "access without action" because the personal information, the private information has been accessed but no action was taken against most of the individuals whose information was seen.

I would hasten to point out that there were some happy aspects of this incident. I might just observe that in such a system hundreds of people will keep hundreds of messages, so there are tens of thousands of messages. Of those tens of thousands of messages in this particular system, there were only two out of order. One was a babysitter's phone number and the other was a cooking recipe for something or other.

The odds are, I would note, that these two items of information, admittedly personal, were probably delivered with less diversion of resources from the job by electronic mail than if the individuals in question had made a phone call or gotten up and walked to somebody else's desk.

I also would salute the management of that agency, whose discipline is so tight that out of tens of thousands of messages in the system there were only two out of order. And I would certainly acknowledge the integrity of those hundreds of people who used it and used it properly.

Let's proceed with its examination by considering the possibility that an agency of Government would decide to use a commercially provided electronic mail service or, for that matter, a private corporation would make such the same decision.

For this argument, let's assume that the computer host that would supply the mail service is out of State. There is no question that electronic mail is an efficient mechanism to facilitate the conductor business in any large organization. That is not the issue I am addressing.

What I would like to suggest, though, are the risks that are involved in proceeding in that direction under some circumstances. And while the technical arrangements are obviously vague and not known, one can make some considered observations. Importantly, these observations would not be limited to any one vendor of electronic mail.

I would note, first, that it is very unlikely that the telephone lines between Washington or the site of the private organization and the other State in which the electronic mail service is hosted, it is unlikely that those telephone lines are protected by encryption. So, electronic eavesdropping and wiretapping of all that mail traffic is perfectly possible.

Second, I would note that it is very unlikely that the computer system hosting the mail service would have any special security safeguards because normally the run-of-the-mill commercial systems are used for such services. One would assume, though, that the vendor did provide the normal, appropriate, physical, administrative, personnel safeguards.

I would observe next that since the electronic traffic flows across State lines that it would be a matter of Federal jurisdiction, but there isn't any Federal law that really accommodates the issue. The information would be largely unprotected.

In principal, the body of information in this example that I posed would be subject to the same seizure as the office workers example. The company would certainly—would simply have no legal standing to resist.

And while I would not suggest for a moment that some agency of Government would seek the electronic mail records of some other agency of Government, a dissident group might, and any such body of mail information might get caught up in an investigative sweep aimed at someone else.

And why do I put all this emphasis on the security and privacy aspects of electronic mail? First, it is coming and coming fast. But second, it has an attribute that is normally overlooked, and I want to stress it.

You must not think of electronic mail as solely the electronic analog of an envelope. Perhaps a fourth of my own business is conducted electronically, and at the moment there are some 600 messages in my electronic mailbox, and it can be as high as a thousand.

And why such big numbers? Because it represents the written record of my conduct of business with a variety of individuals and organizations, and the whole thing is much more efficient than writing letters, making phone calls, and then writing memoranda of agreement—memoranda of record.

Moreover, I can organize all of those messages into folders and files, and so the system becomes a comprehensive, automated, file system with information retrieval. Anybody that had access to that body of information might as well have access to my office safe combination and everything that's in it.

But the point is that such comprehensive business record service is what electronic mail is really all about, and it will be the service to be offered by the private sector. It is the service that the MCI's and the GTE's and the others will eventually get to, and it is the service that the various telephone companies will eventually get to as well.

Now, can you imagine the situation with all that information, both private and corporate, gets into electronic mail systems unprotected by law? Can you imagine what a lucrative target it will become for all sorts of reasons that we can imagine? My view is that the computer matching that we have seen so far will be nothing compared to what might arise when somebody thinks about comparing files from electronic mail systems.

Now here are some of the issues that surround that matter. It's not clear who owns information in an electronic mail system. Does the owner of the computer system own it? Does he have the right to witch hunt through that information as he sees fit? It is not clear if or by what law it is all protected.

What is the situation for intrastate offerings versus interstate offerings and in the long run international offerings? What is the search and seizure situation? Can the private vendor be given legal standing to resist? What's his obligation to his users in case of attempted seizure?

What's his liability in case the system misbehaves and loses mail records? What's his responsibility in case the system improperly spills information to a wrong party? What's his responsibility if maintenance people see that information and use it for private gain or political advantage or private harassment or whatever?

What are the vendor's obligations to provide comprehensive safeguards? Should they be mandated by law? Should they be caveat emptor? What should that all be? Should the Government be concerned that so much corporate information might be subject to penetration by unfriendly agents?

What should be the privacy protections of electronic mail? There have gradually arisen some with respect to telephone billing records. Should we extend the same kind of umbrella of protection to electronic mail?

And I would point out that this is only the beginning because behind electronic mail becomes voice mail, which will have all of the same attributes, plus some additional ones, such as ready recognition of the speaker.

There are a host of other services, some of which were ticked off in the chairman's opening messages: Point-of-sale systems, debit card systems on vendor's—on merchant's premises, a whole host of them having similar situations and similar risks for exposure of private information, but the electronic mail one is upon us now and coming rapidly.

The future of privacy has a lot of dimensions, and that is a once over lightly, a bit of a teaser on it with one dominant issue identified. Now let me wind up by speaking briefly to the issue of a national commission, which has been suggested to you by two witnesses as a mechanism for examining computer crime.

A year or so ago I suggested a national commission to look at the vulnerability of our country as a result of its high level of computerization. The fact is there are a whole collection of issues that are all interrelated, and they are all kept together by the common element of computer technology and communications technology.

It's information handling in the large sense. Included would be computer-related crime, new dimensions of privacy, the national vulnerabilities, representation of information, intellectual property, the concepts for that, social consequences of computerization, personal identification issue—that one is about to be on us again, I think—dislocations of power, and on and on and on.

So, my view would be that a national commission is warranted not for just one small item, but for this whole large collection of highly related and substantive topics.

My personal experience with the Privacy Commission did persuade me that a congressionally chartered commission is an appropriate mechanism to address broad issues of this kind that transcend not only jurisdictional boundaries of Federal agencies but also transcend public and private sector interests.

Congressman Glickman, I really have presented to you this morning a very hurried, once over lightly characterization of a very complex and intricate issue. I will obviously be glad to elaborate on any of these things as you wish in the future.

If Congress has the will to pursue this issue and to pay sufficient attention to it, then I think the time is right to get on with it. And I would suggest, to begin with, that we ought to get GSA in gear, we ought to put ICST to work, we ought to address the electronic mail issue as the most pressing of the new dimensions of privacy, and we might think about making 1984 as the right year to launch a commission to examine this comprehensive set of issues.

Thank you for inviting me this morning.

[The prepared statement of Mr. Ware follows:]

11/3/83

Testimony of

Willis H. Ware

INFORMATION SYSTEMS, SECURITY, AND PRIVACY

Before the Subcommittee on Transportation, Aviation and
Materials, Committee on Science and Technology, United
States House of Representatives[1]

October 24, 1983

INTRODUCTION

My name is Willis H. Ware. I am a member of the Corporate Research Staff of The Rand Corporation, but the views I state today are solely my own; they in no way reflect a position of The Rand Corporation nor of its research clients. Furthermore, my views do not come from a specific contract, but rather reflect a decade of my attention to the issue. I am an electrical engineer by training, but have specialized in the field of computer technology for over thirty years.

My credentials for addressing the issue include the following. In 1967, I was the first to bring the issue of computer security to the attention of the technical field by organizing a special session on the subject at a Joint Computer Conference in the spring of that year. Subsequently, I chaired a Defense Science Board (Department of Defense) committee to look at the issue of computer security which had never been examined comprehensively anywhere in government. The report was a definitive treatment of the subject, and to this day remains an excellent primer. I have furnished three copies of that document to this committee as background information.

---

[1] Additional material on electronic mail was orally presented but did not appear in the originally submitted testimony. This version includes the additional material and has been slightly edited and annotated.

Because of my work in computer security, I was asked in the early 1970s to join a special advisory group to the Secretary of HEW, and I subsequently became its chairman. Its report, *Records, Computers and the Rights of Citizens,* was the first comprehensive treatment of the matter at the federal level. It provided the intellectual foundation for the Federal Privacy Act of 1974, which among other things created the Privacy Protection Study Commission of which I was a member and vice chairman.

In addition to my participation in the activities noted above, I have also spoken and written widely on the subject. In particular, I presented a paper, *Policy Aspects of Privacy and Access,* to a National Science Foundation symposium. Although the paper will be published by Crane-Russak as a special double issue of its journal *The Information Society,*[1] I will forward three copies of it to the committee for background information.

STATEMENT

Congressman Glickman, it is a pleasure to have been invited here today to talk with you about a subject that is of such importance, not only to me professionally but also to the country. Since time is limited this morning, my presentation will be in the nature of a hopscotch over a variety of points and ideas that I think will be of significance for you. I will elaborate or expand in any detail at your request or on another occasion.

Let me first clarify the relationship between security and privacy, where I use the latter term in the context of record-keeping privacy; namely, the use of information about people to make decisions and judgments about them. Record-keeping privacy concerns personal information kept in computer-based systems, and the essence of it is protecting such information and controlling its use for authorized purposes. In contrast, computer security is that body of technology, techniques, procedures, and practices that provides the protective mechanisms to assure the safety of both the computer systems themselves and the information within them; and, in addition, limits access to such information solely to authorized users. Computer security is of importance whether the information to be protected is personal in nature and therefore relative to privacy; whether it is defense in nature and therefore related to the security of the country; or whether it is sensitive in nature and therefore relevant to corporate welfare in the private sector. The important point to be noted is that a comprehensive set of security safeguards within and around a computer-based information system is an essential prerequisite for assuring personal privacy. To operate such a system without relevant safeguards is a sham against privacy assurance.

---

[1] Issue 3/4, Vol. 2 is in press. Anticipated date of publication December 1983.

The computer security issue must be seen as analogous to the classical offense/defense situation. As computer security safeguards become stronger, the offenses against them will become more sophisticated and the cycle will repeat. Therefore, no organization or Congress can assume that the computer security issue is one that can be looked at and forgotten. It first surfaced on the professional scene only fifteen years ago; we are still low on the learning curve with regard to knowing how to incorporate comprehensive protection mechanisms in our systems. It is an evolving issue, not a static end-of-the-road one to be dismissed. Therefore, I would recommend to you that:

> It be a standing agenda item for this or other committees of the Congress to look at every year or so for at least the next five and possibly the next ten years.

Next, let me contrast the security situation in the defense environment versus that in the commercial/industrial world. Within defense the threat against computer-based systems includes the full technical resources of advanced major world powers, where such threats can be mounted with substantial funding and other resources. In the Department of Defense context, therefore, the threat includes intense technical aspects as well as aspects involving people -- such as buying them for subversive actions. On the other hand, the defense community does go through an investigative process to grant formal clearances to people; therefore, it has substantial assurance of trustworthiness.

In the commercial sector, on the other hand, the technical threat is at present minimal. The big threat is people within the systems themselves. If one examines, for example, the Parker/SRI database of computer-related criminal actions, he finds that the great bulk of them have been perpetrated by an individual who was authorized to interact with the system and who knew enough about it to exploit it for personal gain. Furthermore, there is generally little attention paid in the commercial world to establishing trustworthiness of individuals in critical and sensitive positions within a computer-based information system. Some corporations do essentially nothing by way of assuring the trustworthiness of critical individuals; others take the minimal step of requiring that individuals be bondable -- a really minimum level of assurance of trustworthiness; and very few, perhaps none, engage in a comprehensive background investigation. When the private sector gets the "people problem" dimension of the threat against its computer systems under control, and the simple technical threats protected against, then sophisticated technical threats will become more important.

Let us examine the last point more closely. What can we do about the simple technical threats, such as those used in the Milwaukee-414 caper, or those involved in the various criminal acts of the SRI database? The dominant point is: technology is not the issue. There are ample technological safeguards that can be installed, and would be effective against many of the crimes that have been perpetrated and against many of the mischievous pranks that have occurred. There are also procedural and administrative safeguards that can be important deterrents. In the private sector, we need only the corporate will to address the problem, and the corporate commitment to put the issue on the same level of concern as that of protecting other valuable resources. By implication, we also need the corporate commitment to spend the modest sums needed. Importantly, we need private sector users of computers to signal the computer industry that technical safeguards are wanted, are essential, and will be paid for.

Do not underestimate that last point. Until the IBMs, the DECs, the Burroughs, the UNIVACs, and others of the commercial computer industry understand that their respective customer bases want technical security safeguard features, the product lines will not have them. I would suggest that the government has a major leverage on this issue. It can make mandatory the inclusion of appropriate technical security features in computer systems that it procures.

Consider now the people aspect of the threat. It is a hard one to counter because one cannot legislate trustworthiness, and even the most extensive background investigation may not reveal deeply hidden or latent problems. To start with, we must do all that is possible with technical procedural safeguards; a good array of them will fend off many people problems. We might take legal steps. One possibility for encouraging private sector response would be to create a basis in law for acting against the record-keeping installation for contributory negligence should state-of-the-art security safeguards not be in place.

It might be possible to extend the principle of the attractive nuisance, which in a sense is really what happens with 414-type activities. A computer system is not a physically attractive nuisance, but rather an intellectually attractive one that causes imaginative or criminally minded people to hack at computer systems. The legal principle of an attractive nuisance encourages people to build fences around swimming pools; perhaps the same notion can be elaborated or reinterpreted to encourage operators of computer systems to install appropriate safeguards.

Incidentally, for the most part we are not talking about large dollar investments. Clearly, if an organization operates its computer center behind a plateglass window and encourages casual visitors to wander among the equipment, there might be a significant initial investment to physically secure the facility and provide it with appropriate physical and fire protection. Beyond this phase though, many organizations find that important security safeguards can be installed as part of changes that are made for other reasons and the costs of such security changes are frequently unnoticeable. Cost will not be zero but neither will it be burdensome.

What about technical safeguards against the people threat? There are attractive options and I will illustrate with two examples. When an individual logs on to a computer system, he is normally requested to supply personal identification and a password which, in effect, is an authentication of his identity. Someone attempting to penetrate a computer system tries to guess his way in by masquerading as a legitimate user. Most systems today permit an indefinite number of log-on trials. It therefore is feasible for a perpetrator to program a small computer to systematically try words, combinations of letters and characters, or other possible passwords until one is found that works. The movie *WarGames* showed such a penetration very realistically and accurately.

Clearly, this is an undesirable and unsafe arrangement. There is no reason why a computer should not disconnect an individual after some number of attempts, such as three or five, and keep him disconnected until his authenticity has been assured. Three weeks ago you heard from Mr. McClary of the Los Alamos National Laboratory. He did not mention the arrangement at Los Alamos with regard to passwords, but since I happened to have discussed computer security with LANL recently, let me indicate how it is handled.

If an individual -- and it might be a respected, established senior researcher of national repute -- fails to log on after a number of tries, such as three or five, his account is completely disabled until he personally appears at the security office and explains why he was unable to type his password successfully after the prescribed number of tries. If he fails to log on successfully in a second series of attempts, his supervisor is required to explain in writing why the individual in question seems not able to type correctly. While this process might seem stringent and it is undoubtedly annoying to an individual, nonetheless disabling repeated log-on attempts is an appropriate arrangement to fend off penetration attempts by guessing in. The media reported the Security Pacific National Bank as having diverted a presumed penetrator by offering him a game to play while tracing the origin of the call; such an approach is obviously a very imaginative and appropriate deterrent.

A second example. Since every computer system has to be started at some time, invariably there is a mechanism for accomplishing what is called the initial software load. Often this takes the form of a button, a switch, or a sequence of actions by the console operator. Imagine a scenario in which an operator on the graveyard shift finds the machine inactive and decides to do something in his own behalf such as illegally copying a sensitive file of information. Having done so, he simply reloads the machine as though it had stopped for some reason; there will be no record of what he has surreptitiously done. There are obvious technical offsets to such malfeasance by operators, but they do not exist in marketed machines. Even the procedure of two-person control as used by the military would be a deterrent.

We need a menu of technical features that machines should have in order to help offset aspects of the people-threat problem. Let me offer you a recommendation:

> Task the Institute of Computer Science and Technology of the National Bureau of Standards to produce such a list of options, and consider making it mandatory in government acquisitions of computer systems.

Now to the question of where the wisdom will come from within government to deal with the broad dimensions of computer security. I remind you that there are technical aspects of it related to not only hardware and software but also to communication security and radiation security (TEMPEST); but in addition there are physical, procedural, personnel, and administrative aspects. Every one has to be attended to, especially the last three. A computer system with the best technical safeguards can be readily penetrable if it is operated with sloppy and careless procedural and administrative arrangements by people with uncertain backgrounds. Where will the government develop the guidance that it needs on these many dimensions?

Many of them are already in hand because they are understood for other reasons. For example, the Department of Defense certainly knows how to deal with physical security and with personnel security; its experience is available to other agencies of government as might be needed. The TEMPEST radiation issue is understood and safeguards for it exist. There are many private organizations today that can advise on fire protection, physical protection, personnel control, and the likes. But, in government where does the technical software/hardware guidance come from? And where does the contextual administrative and management guidance come from?

What are the government's principal assets? You heard from them on October 17; the Institute of Computer Science and Technology of the National Bureau of Standards, the Computer Security Center of the National Security Agency, and GSA. Take the CSC first.

The focus of concern in CSC is "trusted systems" and especially "trusted software." Understand the word "trust" as you would intuitively think of it; namely, one can have confidence that the system or the software will do what it is supposed to do, and one can have confidence that it will not do what it is not supposed to do. Keep in mind that CSC is a Department of Defense entity, and therefore its focus of concern is on defense systems and especially with a sophisticated technical threat. It can and it will provide expertise to address the software/hardware issue.

I suggest to you that the problem of incorporating security safeguards in software -- and of knowing that they are really there and functioning correctly -- is so difficult technically and the country's expertise is so miniminal on it, that we can staff only one such Center at the moment. We would be wise to place all our eggs in this one basket with regard to trusted software until additional expertise can be developed over the next five to ten years. While CSC will also be concerned with other security aspects of systems that contain both computers and communications, it will not be concerned with the general administrative and procedural environment in which secure systems must be operated.

The ICST of the NBS is also involved in technical work. For example, it was the source of the Digital Encryption Standard some five years ago and it made a very significant contribution to the protection of information while in transit through a communication network. It also publishes the *Federal Information Processing Standards* which deal with such issues as the use of DES, the management of keys for it, risk assessment and risk management. But, neither the ICST nor the CSC is providing the comprehensive overview that can stipulate:

- Here is how one runs a computer system and does it securely.
- Here are the procedural and administrative safeguards that must be in place.
- Here are the specific risks that people represent.
- Here are the countermeasures that can be taken against the nontechnical threats.
- Here are the management mechanisms to oversee security safeguards.
- Here are the general protective precautions that can be taken. Etc.

No entity in government has addressed the general policy issue of what constitutes a comprehensive top-to-bottom prescription for installing security controls, nor identified the many dimensions of such a policy and made it available as guidance. It is being done piecemeal; every agency is inventing it for itself or not doing it. There is some policy guidance in the DoD in the form of general regulations and directives. There are interagency committees and technical organizations in which people can trade ideas and talk with one another. In the private sector, major corporations have built their own policy structures and implementing details.

The government truly needs a comprehensive "how to do it" document that sets forth preferred practices and procedures for operating a secure computer system. The private sector could well use the same thing. The ideas and the information exist but everything is scattered. The information is not collected and coordinated; it is in people's heads or embodied in daily activities and not otherwise documented. We -- the country -- need to organize the collective wisdom of what is known and what is being done and make it widely available.

As a first step, I would note that the General Services Administration has had a major role in government, and it therefore seems reasonable to recommend that:

> You task the GSA to compile such a comprehensive handbook of preferred practices and procedures for running a computer center securely.

It is not a big undertaking. It is not an endeavor for tens or dozens of people working for many years. One could survey the federal agencies and a selected set of large corporations, assemble the composite wisdom of what is being done and what is known, and get it written down. I would submit that it is a chore for a few people for a year or so.

Mr. Stephen Walker testified before you on September 26 and suggested a Federal Center to undertake some of the tasks that I have suggested above be done by ICST and the GSA. Such a Federal Center would undoubtedly be a good idea and we clearly could well have one in the long run. CSC cannot do everything; moreover, some of its technical knowledge can never be shared because of national defense reasons. But in the large, CSC represents an innovative opportunity for interaction between the federal government and the commercial sector. It can respond to technical issues and it can examine and certify commercial software products for trustworthiness; but CSC is not likely to concern itself with the less esoteric and more mundane issues that a Federal Center might accommodate. Until, and if, we get such an organization in place, however, there is no reason why the ICST and the GSA ought not do what clearly can be done now.

I do not want to conclude this testimony without touching briefly on privacy. First, let me clarify a statement which I believe was made to you by Congressman Wirth. I disagree strongly with his observation that all the aspects of privacy have now been attended to. In fact, most of the recommendations that were made by the Privacy Protection Study Commission have not been implemented in law, and moreover there are new dimensions of privacy that the PPSC did not identify nor treat. To date, privacy has been interpreted in the context of record-keeping processes, but it is clear that the widespread application of computer and communication systems to provide a broad spectrum of services will eventuate in many new dimensions of privacy.

We are seeing the emergence of systems that contain vast amounts of information about people but not for record-keeping purposes. Let me illustrate in terms of electronic mail, which the U.S. Postal Service is promoting as E-COM. The purpose of such a service is to transport information from sender to addressee and to the extent that such information is personal in nature, the system will contain much information about people but not for record-keeping purposes. In addition to the message content, the system will contain information relating addressee to sender. In principle, such information could be used to establish relationships among groups of people, such as organized groups or circles of acquaintance. Obviously, such information could be of high interest to the law enforcement community and others, but the legal umbrella of protection over it is confused and probably incomplete.

Whatever one believes about the security of information in the hands of the USPS's E-COM, it is clear that private offerings of electronic mail, such as by MCI and GTE, are another question. In the case of the latter there is little, if any, legal protection for message information in the hands of private organizations.

I will develop the issue more fully with two examples relative to electronic mail. In a federal agency, the in-house investigative staff on at least three occasions obtained a complete printout of the electronic mail system that provides office-automation support. On at least one occasion, an outside law enforcement entity was also involved. In effect, several hundred workers who use electronic mail in the conduct of their business had all their computer records read; and in at least one instance, an indvidual was intimidated. The privacy of the workplace records of hundreds of people had been invaded; hundreds of people were caught up in an investigative sweep without recourse to protect themselves.

It all sounds very much like search-and-seizure without due process of law, or like a fishing expedition to see if something wrong had happened or if some crime had been committed. In this instance, the computer happened to be agency-owned; one wonders what the situation might have been if the mail service had been provided by a commercial vendor whose computer would be located on private premises?

I do not know the motivations of the investigative groups; I have only one side of the story. Perhaps they were tracking down hackers, or maybe it had to do with possible fraud or embezzlement. I have no wish to make this incident a cause celebre, but it is very useful to underscore the ease with which new privacy issues arise as computer and communications technology is exploited to provide a wide variety of new services to a wider and wider population of users.

It is an example of a new dimension of privacy -- "access without action"; computer matching of files exhibits the same dimension. Individuals who happen to keep records in a computer system or who are record subjects in a computer file have their privacy invaded whether or not an individual has done something wrong. Private information gets exposed to a third party and possibly to hostile eyes. In effect, all the hundreds of office workers or all the data subjects in a computer file have a priori been assumed to be guilty; the examination of mail or the matching of computer records is to demonstrate that they are not. Much information about people has been seen but no action taken. It sounds like a back-end-to process of justice.

There are some happy aspects of the office-automation seizure. In such a system, hundreds of people will keep hundreds of messages each; there will be tens-of-thousands of messages altogether. Only two aberrant ones were found: a baby sitter's phone number and a cooking recipe. The odds are that each item, admittedly personal, was transmitted more efficiently by electronic mail than by a phone call or a walk to another person's desk; the electronic mail system surely diverted much less people time from the job than any other means of interpersonal communication.

Certainly there are management problems in assuring that corporate or business resources are not used for personal reasons, but I salute the management discipline of an agency that operates such a tight facility -- two items out of many tens-of-thousands is really an infinitesimal ratio; and I acknowledge the integrity of the hundreds of people who are using it.

Let us examine the possibility that an agency of government were to use a commercial electronic mail service which is supplied by a computer host that is most likely not in the District.[3] There is no question but that electronic mail is an efficient mechanism to facilitate the conduct of business in any large organization; that is not the issue. What are the risks to such an arrangement? I can offer some considered observations -- which importantly would not be unique to any one private sector vendor.

- It is unlikely that the phone lines whether dial-up or dedicated between Washington and "the other state" would be protected by an encryption process. Electronic eavesdropping and wiretapping would therefore be possible threats.
- It is unlikely that the computer system would have special security safeguards because commercial equipment is often used for such services. One would assume that the vendor has provided appropriate physical, admininstative, and personnel safeguards.
- Since the electronic traffic would flow across state lines, it becomes a matter for federal law; but there is no law under which the information would be protected.
- In principle, the body of computer-contained electronic mail would be subject to the same seizure as the office workers experienced; the private vendor would have no legal standing to resist. While I would not suggest for a moment that some agency of government would set out to seize the electronic mail of another, a dissident group might and such mail could get caught up in an investigative sweep aimed at someone else.

---

[3] After the presentation of this testimony, the author's attention was called to a *New York Times* article (July 13, 1983, Late City Final Edition, page 18, section A, column 4) which describes the Executive Data Network which provides the Executive Branch of government with electronic mail services from a system in Columbus, Ohio. The article also reported by name the officials who were to use it.

Why all my emphasis on both security and privacy of electronic mail? You must not think of electronic mail as solely the electronic analog of the envelope. Perhaps one fourth of my business interactions and transactions occur electronically; at the moment there are about 600 messages in my mailbox and it can get as high as a thousand. Why? It represents the written record of my conduct of business with a variety of individuals and organizations; it is much more efficient than writing letters, making phones calls, and then writing memoranda-of-record. Moreover, I can organize the messages by folders and subfolders so that the system becomes a comprehensive automated filing and information retrieval system. Anyone having access to such a body of information might as well have the key to the office and to its file cabinets.

Such comprehensive business records service is what electronic mail is really all about, and it is the service that will be offered by the private sector. Can you imagine the situation when all that information -- both private and corporate -- gets into electronic mail systems? Can you imagine what a lucrative target it will become for all sorts of reasons? The computer matching we have seen so far will be nothing compared to what might arise when someone thinks about comparing files from electronic mail systems.

Here are some of the issues for information in such systems:

- It is not clear who owns it. Does the owner of the computer system per se own it? Does he have the right to witch-hunt through the information in his system as he sees fit? Or is asked to by a third party?
- It is not clear if, or by what law, it is protected. What will be the situation for intrastate offerings of service vs. interstate offerings? And in the long run, for international offerings?
- It is not clear what the search-and-seizure situation is; can the private vendor be given legal standing to resist? What should be his obligations to the users of his system in case of attempted seizure?

- It is not even clear what the liability of the purveyor of the service might be, should something happen to one's electronic mail records. What is his responsibility or obligation if his system accidentally spills information to the wrong party? What is his responsibility if his maintenance people accidentally see such mail information and use it for private gain, for personal embarrassment, for political advantage, or for a breach of national welfare and security?
- What are the vendor's obligations to provide comprehensive security safeguards for his system? Should they be mandated by law? Should it be caveat emptor? For private sector and government use alike? Should the government be concerned that so much corporate information might be subject to penetration by unfriendly agents?
- How should electronic mail be treated relative to telephone conversations? Over the years, certain privacy protections have arisen for telephone billing records; formal legal processes are necessary to wiretap or to obtain records. Should similar protections exist for electronic mail? Within government, as well as in private sector, as well as in regulated public utility?

Many of these same concerns will also be pertinent to other systems. For example, there is voice mail which is the spoken analog of electronic mail -- a service which is actively being promoted by private vendors and by various telephone companies. Voice mail has all the vulnerabilities that electronic mail has when offered by public vendors; moreover, an intruder can always claim that a particular individual's voice can be recognized although his typed signature can be forged by someone else at the keyboard. Encryption techniques can be used to protect electronic mail but present systems do not offer sender-to-reader encryption options. It is much more difficult technically to provide speaker-to-listener protection for voice mail.

There is, in addition, the body of information which is collected about people by point-of-sale systems, by debit card systems on the merchant's premises, by automated checkout stands in grocery stores, and a whole host of others. In each case the system exists for some purpose other than the traditional record-keeping one; each happens to contain information about people as a collateral consequence of its primary intent. But the whole subject of privacy ahead, of what the future holds for privacy, of what its new dimensions are, is for another day; I have left you just a little teaser of what it will be all about. Clearly, electronic mail is upon us now.

Let me speak to the issue of a National Commission. Congressman Wirth and Mr. Parker suggested to you on September 26 that a national commission to investigate computer crime would be appropriate. A year or so ago I suggested at a National Computer Conference that a National Commission would be an appropriate forum in which to examine possible vulnerabilities of our highly computerized society. The fact is that there is a whole set of interrelated issues that could well be collectivly examined by a congressionally chartered commission. The common element to all of them is information handling as performed by computer and communication systems. Included would be such things as computer-related crime, new dimensions of privacy, national vulnerability as a result of computerization, representation of information, social consequences of intensive computerization, personal identification in a highly automated society, dislocations of power as a result of concentrations of information, and others.

My personal experience with the Privacy Protection Study Commission persuaded me that a congressionally chartered commission is an appropriate mechanism to address broad national issues that transcend the jurisdictional boundaries of federal agencies and also transcend public and private sector interests. Such a commission can provide an enormous bargain for the country in terms of work accomplished. For example, the PPSC delivered about 60 man-years of research on the subject of record-keeping practices in the private sector for about $2.5 million. That equates to about $40,000 per person-year of effort which is about one third of what it would cost if done by a contractor. In my view there is a right and a wrong way to structure a commission, but that is a subject for another time if the Congress should be persuaded to move that way.

Congressman Glickman, I have given you a once-over-lightly on some aspects of a very intricate and complex issue. I would be glad to deal in more depth with such aspects as you may wish, either in writing or personal discussion with your staff. There must be a national concern for providing adequate security protections in our public and private information systems and for attending the new privacy issues that arise. We know a lot about doing it, but it needs to be organized into a concerted effort. If the Congress has the will to pursue this issue and to pay sufficient attention to it, my feeling is that the time is right for action.

To begin with, let's get the GSA going; let's put ICST to work; let's address electronic mail as the most pressing of the new dimensions of privacy. Let's think about making 1984 "the right year" to launch a Commission to comprehensively examine the many issues of which we have talked.

[At the conclusion of the testimony and questions, the chairman, Congressman Glickman, read excerpts from a *New York Times* article (Sunday, October 23, 1983, page 21). It described the penetration of the Telemail service offered by GTE, and the apparent access to the electronic mail of major U.S. companies such as Raytheon, Coca-Cola U.S.A., the 3M Company, and of several federal agencies such as NASA and the Department of Agriculture.]

Mr. GLICKMAN. Thank you for an excellent statement.

I would like to pursue several items. One, though, before we begin, was a reference that you made in your statement to a law enforcement agency or group that was penetrating or might have been penetrating the electronic mail service of Government workers.

And I was kind of reading something and then I—it hit me, went in one ear and out the other, and I thought you might perhaps want to expand on that a little bit. What you said, is what I am saying, repeating what you said.

Mr. WARE. This incident was described to me, as a matter of fact, in electronic message it came to me over the ARPAnet. I made point to track down the source of this information over the weekend. He said that it would be acceptable to him and his management to describe the issue, so to speak, anonymously. Whether on subsequent circumstances one can get deeper in identification remains to be seen.

The matter simply was that on three occasions the internal investigative forces—I don't know whether they are called the IG's or the whatever—arranged for complete printout of the electronic mail records of that computer. And on at least one of the occasions the internal investigative force was accompanied by an external but still Government-level investigative group.

Mr. GLICKMAN. Do you know what they were looking for?

Mr. WARE. No, I don't know what they were looking for. I obviously have only one side of the story, and that's why I didn't want to blow this up into a—into an incident out of proportion.

Mr. GLICKMAN. But you are trying to discuss the potential for law enforcement officials to get into electronic mail and review what is being written.

Mr. WARE. Yes, and the fact that that—and the fact that such information in that instance at least was presumed to have been the property of the agency who owned the computer.

Mr. GLICKMAN. And you don't know whether this was done to, let's say, do oversight over the content of Government mail that was done by their employees or whether there was an impending investigation going on?

Mr. WARE. I do know that this was not a usual job monitoring service. This wasn't the telephone operator listening in to make sure that service was OK. It wasn't that kind of an example. It appears to have had some kind of investigative overtones, but details of that I don't know.

Mr. GLICKMAN. You raise the issue of job monitoring and telephone monitoring, and I think that this would be a subject that I would like to pursue at some point in time because obviously not only does the Government have that capability from an oversight point of view, but I would hate to see the FBI without a search warrant doing this kind of thing because it would be the same—obviously the same situation, would it not, as it would be wiretapping from the purposes of the law?

Mr. WARE. I don't know. Just answering you off the top of my head, I don't know whether I would want to draw that analogy.

Mr. GLICKMAN. Well, if the Government were to access itself into an electric—let's say the FBI into electronic mail processing or records of parties under investigation for a crime without a search warrant, it would seem to me that there would be a lot of parallels to electronic eavesdropping.

Mr. WARE. I agree with that analogy, and that's really the whole issue, the protection for that information, what legal process is warranted to have access to it.

Mr. GLICKMAN. And you are saying the law is very undeveloped in this area, as well as the practice of people in the industry.

Mr. WARE. Well, I am not a lawyer, but I would say it is stronger. It is not only undeveloped, it is absolutely absent.

Mr. GLICKMAN. OK, that is a fairly strong statement.

I think that your idea of asking the GSA to compile a comprehensive handbook of preferred practices and procedures for running a computer system and the security relating thereto is a good idea.

Have you made that suggestion to the GSA before?

Mr. WARE. No, no, I haven't, but I know Frank McDonough and Frank Carr down there. And they may not take kindly to that suggestion, but they are up to doing it.

Mr. GLICKMAN. Well, the reason why I mention that is because we had Government officials in. We didn't have the GSA in, but we had OMB, and OMB theoretically assumes for itself kind of the policy leader in setting guidelines for the government in this area.

I wonder if you might comment on how they are doing, should OMB be taking a more forceful leadership role in providing the kind of guidance that you list in your statement, and—or should the GSA be doing this independently or does it matter?

Mr. WARE. The first issue, the prominent issue, first and foremost, is to get the leadership. The second question is where does it come from. Now, the OMB got it because of a law, what is it, about 2 years ago, that establishes this whole information resource management business, gave that obligation to the OMB.

I wouldn't be prepared to argue one way or the other as to whether the OMB is the right place, but I would be prepared to argue that somebody's got to be the right place. I would suggest that government ought to figure out which is the right place and make it happen.

Mr. GLICKMAN. Do you think that the insurance industry has a role to play in elevating private sector concern with computer security? You talked a little bit about—well, the common law may be changed to making it a common law tort, so to speak, to if you don't take the appropriate security controls you could be subject to lawsuit. I am wondering if you could take that further, in saying that the insurance industry ought to maybe base their rate premiums in this area on what kind of security mechanisms are in place.

Mr. WARE. Well, I am a little puzzled by that because for the most part the insurance industry runs their own in-house computers, so the whole security issue is within their own hands.

Mr. GLICKMAN. Well, I am talking about insuring other companies.

Mr. WARE. Oh, I understand.

Mr. GLICKMAN. Let's say that—I am not going to insure the Master Charge Co., period, unless they have a variety of other, you know, security measures.

Mr. **Ware**. Yeah, that is an interesting idea. That is a bit of leverage that one might use, yes.

Mr. **Glickman**. On electronic mail, what problems are there in placing security controls and why is it difficult to place controls?

Mr. **Ware**. Security controls and electronic mail systems are no different than security controls in any other computer systems. It's just we got to get busy and do it.

Mr. **Glickman**. There is nothing unique there in terms of the technology or the management systems?

Mr. **Ware**. There might be a few things that are special and unique on the edge, but for the most part it is the same body of technology, the same body of wisdom.

Mr. **Glickman**. OK.

Mr. McCandless?

Mr. **McCandless**. Thank you, Mr. Chairman.

Dr. Ware, I was fascinated by your opening comment about there needs to be a corporate commitment, a corporate will in the field of the security aspect of it. I am reminded of one of the famous cases out our way, Security Pacific, and the fact that as I pass up and down the street in my district and a new savings and loan is built or a banking institution is built, we have this great complex thing being built first and then the building is built around it, and then when it is completed there is a door multiple feet thick for the purposes of security.

And yet, we are saying here that the same institution does not take comparable measures in areas that would be supposedly comparable to the actual dollar and its presence on the premises.

Can you expand a little bit on that? I——

Mr. **Ware**. Well, first of all, I would want to be careful to point out that some industries are better than other industries.

Mr. **McCandless**. I am sorry, I didn't——

Mr. **Ware**. Some industries are better than other industries with regard to their attention to this whole matter. The financial community for the most part is in reasonably good shape, but I think for a very good reason.

Ever since the boys with the black hats and the guns robbed stage coaches, the financial community has understood the necessity to protect valuable resources, and they have been doing it. And so, they have incorporated that mind set, that philosophy, that attitude, that point of view toward their information systems as well.

So I would say that the financial community, to the extent that I know its details, is in reasonably good shape with regard to security controls. That is not to say that there are not loopholes. The people still open safes, too, so there isn't any absolute, and events will take place and computer systems will be penetrated and safes will get opened.

So that is the point of my observation about offense/defense. As fast as we find the loophole, we fix it, but then some ingenious soul finds another loophole, and then we fix that.

But the insurance community I would think in the large is in pretty good shape because they are protecting highly competitive assets. The financial community I would think is in pretty good shape because they are protecting assets and they have obligations to regulatory agencies. So it is a very spotty attention that is being paid out there, with some communities being much better off than others.

Mr. McCandless. In the field of defense or defense-related institutions, industries, what is your observation relative to their level of security?

Mr. Ware. Well, since the DOD in its contracting process lays very rigid rules on how all of us behave with the material of defense nature, those—those circumstances are, generally speaking, excellent. But once again, that is not to say that things won't happen from time to time.

Mr. McCandless. Then where is the commitment and the will needed, where is it sorely lacking in the current structure?

Mr. Ware. It's all of those places that I haven't mentioned. It's all of those places that are getting a hold of information about people that they have never had to deal with before. It's those places that have never had high on their list the attention required to protect valuable assets.

Mr. McCandless. The competitive marketplace where one might get a leg up on another one by tapping that type of thing?

Mr. Ware. For example. Now, the petroleum industry understands very well that data that comes out of oil wells and production rates and all of that is very important but, at the same time, in one instance that I know of it chose to use an electronic mail service for something which I would have regarded personally as highly risky.

But more to the point, the decision to use that electronic mail service and an evaluation of its risk versus value was not made at the corporate level. It was made about four echelons down in the structure. To me, that is not an exhibition of high concern for the whole question of information protection.

Mr. McCandless. This point that the chairman covered about the handbook with respect to governmental agencies, I am assuming that there are in certain locations within the governmental structure existing handbooks created by that institution or agency for its own use. Have we seen any of those?

Mr. Ware. I would assume, as you did, that some of those exist, but I don't have a library of them, nor have I ever seen them. Now, there are regulations that exist, but it is not—the regulations and the policy are one aspect, but it's the implementing detail that we need to pull together.

Mr. McCandless. Now, could we take an overall handbook and apply it to the Department of Transportation the same way we would apply it to health and human services and then turn around and do the same thing over at Housing and Urban Development?

Mr. Ware. In the large I would think the answer is yes. There may be special items out on the edge that you would have to worry about, but in the large the principles will prevail.

Mr. McCandless. So there are common denominators within the total structure that could apply?

Mr. Ware. A computer system is indifferent to whose information it is processing. It doesn't matter whether it is HHS or DOT or electronic mail or anything else. You can lock it up, you can protect it, you can control access to it. The computer system doesn't care.

Mr. McCANDLESS. The thing that is puzzling to me—and I am probably expressing my ignorance—but when the computer was not around, file cabinets were locked, the file cabinets were within rooms and the doors were locked, and people who had access or responsibility had the necessary keys or combinations or whatever it might be to go through the process to acquire the document in question. And if there was to be some legal requirement of the law enforcement agency, wiretapping was authorized by an agency of the government, be it a judge or whatever.

I am drawing here mentally parallels between all of these less sophisticated types of things and what we have now, and I am saying why can't we do a similar thing with respect to who has access to the actual instrument by which they can acquire this? If you are going to tap a wire, you are going to tap a wire. It isn't going to make any difference whether it is a line carrying computer information or a conversation or a voice.

Mr. WARE. That is almost true—that last remark is almost true technically, but it is not important to examine. Part of it illustrates that decades or centuries of experience on the one hand of protecting physical objects versus—I mean, versus, what, 15 years with protecting electronic objects.

Another part of it is centuries of management mind sets that understand—see physical objects and have a great deal of difficulty dealing intellectually with electronic objects. It is an old, established subject on one hand with managers that know what to do about it. It is a very new, fast moving, highly technical subject on the other hand, generally speaking, with managers that are uncomfortable with it.

So, it is a catch up game that we are in, and in a catch up game one looks around, which is what we are all doing, we are looking around for motivations to try to make the catch up go faster.

Mr. McCANDLESS. Thank you, Dr. Ware.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you.

I just would mention one thing. In Sunday's New York Times there is a story headlined "Computer Entries Identified by FBI." I thought I would just read a few paragraphs of it because it goes to emphasize what you are saying.

> The federal authorities engaged in a nationwide investigation of unauthorized entry into computers say that intruders have tampered with the electronic mail of about 18 corporations and Government agencies that subscribe to the same communications service.

I am reading on that the FBI requests an affidavit, searched—four of the corporations are Raytheon, the RADA Corp. Coca-Cola, and the 3M. It said NASA and the Department of Agriculture were among the Government agencies whose electronic mail was tampered with.

I think probably that many of the things you have said today, Dr. Ware, may be understatements and that the problem may become even more severe than your demeanor today would indicate, but I think you have stated the case quite clearly and strongly, and we appreciate your testimony.

Mr. WARE. Thank you. I didn't really orchestrate that news release, but it is very fortuitous.

Mr. GLICKMAN. OK. Thank you very much.

Why don't we put that into the record, too.

[The article follows:]

COMPUTER ENTRIES IDENTIFIED BY F.B.I.—INTRUSION REPORTED IN MESSAGE SYSTEMS OF 18 COMPANIES AND FEDERAL AGENCIES

(By Joseph B. Treaster)

The Federal authorities engaged in a nationwide investigation of unauthorized entry into computers say that intruders have tampered with the electronic mail of about 18 corporations and Government agencies that subscribe to the same communications service.

Spokesmen for several of the corporations said no trade secrets or other sensitive information was transmitted through the electronic mail service that is provided by a Virginia company and that they suffered no significant losses. The service is known as Telemail.

The Federal Bureau of Investigation, in an affidavit requesting a warrant for a search of an office on Long Island, identified four of the corporations that had been victims of unauthorized intruders as the Raytheon Company, the RADA Corporation, Coca-Cola U.S.A. and the 3M Company.

It said the National Aeronautics and Space Administration and the Department of Agriculture were among the Government agencies whose electronic mail was tampered with.

Joseph P. Erb, the chief of the Operations and Telecommunications Division of the Department of Agriculture in Washington, said he knew of no unauthorized entries into the department's electronic mail. But he added, "It's obvious the F.B.I. knows something we don't."

In Atlanta, Dolores Sanchez, a spokesman for Coca-Cola U.S.A., would not say whether there had been intruders in her company's electronic mail. "I can't comment on it," she said.

One Federal agent said that only a half-dozen of the 18 corporations and agencies were named in the request for the search warrant because "these were the ones we pretty much had nailed down. I don't think we have information yet on just what was done with all the others."

However, one of the companies named, the RADA Corporation, was not listed in standard reference listings of American companies, and Federal investigators said they did not know where the company was situated or what it produced.

SEARCH AT STONY BROOK

The affidavit had been used to obtain a warrant to search an office at the FM radio station of the State University of New York at Stony Brook on Oct. 13. In the search a computer and other equipment owned by Frank P. Burgert, a part-time student and part-time engineer at the station, were confiscated.

The raid was one of 15 carried out by agents around the country on Oct. 12 and Oct. 13 in the investigation into unauthorized entry and use of the Telemail service operated by the G.T.E. Telenet Communications Corporation in Vienna, Va. The agents seized thousands of dollars worth of computers and equipment. No suspects were charged, and there were no arrests.

James E. Mull, a spokesman for the Alexandria field office of the bureau, which is serving as the headquarters for the Telemail investigation, refused to comment on the affidavit. He said he understood that all the affidavits for search warrants in the investigation had been sealed and it was "probably a clerical error" that the affidavit in the Long Island search had been made available in the Federal District court in Brooklyn.

In Lexington, Mass., A. Newell Garden, a spokesman for the Raytheon Company, a diversified electronics concern, said his company had lost no data to intruders.

He said Telemail was not widely used among Raytheon's 75,000 employees and that the company had been paying the minimum monthly fee of $500 for the service. In contrast, NASA officials said they had been paying an average of $21,200 a month for Telemail, and Mr. Erb of the Department of Agriculture estimated the monthly bill for his agency at about $5,000.

3M REPORTS NO DAMAGE

In St. Paul, Minn., Pete N. Holste, a spokesman for the 3M Company, the makers of Scotch Tape and dozens of other products, said that at least one of the company's 45 divisions used Telemail extensively and that members of that unit learned of intruders in the system last Monday when they were issued new passwords by the Virginia company.

He said he knew of "no damage at all" and said he did not believe 3M was "terribly worried" about the intrusions.

In Washington, Louis Lushina, who has responsibility for the Telemail service at NASA, said of the intrusions: "I don't think people should feel it's a game."

"First of all," he said, "if people go in and use the system it's costing someone money, either the firm or the operators of the system. It's not a very sensible or appropriate thing to do."

Mr. Lushina said some NASA messages had been destroyed, but he did not know how many.

Besides the raid at Stonybrook, five others were conducted in New York State in Scarsdale, Albany, Ithaca, Rochester and Port Jefferson.

Most of those named in the search warrants were teen-agers, but there was also a 47-year-old clinical psychologist in Council Bluffs, N.Y., and the 26-year-old engineer at the Stonybrook radio station. In Rochester the agents confiscated equipment owned by a young couple and in Ithaca their targets were two Cornell University freshmen.

The investigation was begun Aug. 29 after Telenet told the bureau it had discovered "unidentified intruders" in the electronic mail service it provides to 130 clients.

Mr. GLICKMAN. Our next witness today is Gen. Jack Hancock, senior vice president, corporate strategy and systems for the Wells Fargo Bank in San Francisco. There you are, right in front.

Appreciate your being here today. The committee welcomes you.

STATEMENT OF JACK L. HANCOCK, SENIOR VICE PRESIDENT, CORPORATE STRATEGY AND SYSTEMS, WELLS FARGO BANK

Mr. HANCOCK. I appreciate the invitation, Mr. Chairman.

Let me say that I had asked—while I was in the Army and a retired and I am here not—the title is there. I had arranged at the last minute to have it changed, but your agenda was already printed. So, I am here with you as a representative of Wells Fargo.

Mr. GLICKMAN. We will call you Mr. Hancock.

Mr. HANCOCK. I prefer that, Mr. Chairman, for this purpose. Thank you.

Mr. GLICKMAN. OK. Sure.

Mr. HANCOCK. I'm responsible at Wells Fargo for a function which we call strategy, systems and personnel, and I will elaborate on that in just a moment.

Wells Fargo & Co., of which I am an officer, is the parent of Wells Fargo Bank. Wells Fargo Bank and the company are both headquartered in San Francisco. The bank is the 12th largest in the United States in terms of assets, which are about $25 billion. It's the oldest bank in California. We are a bank which has placed very heavy emphasis in the past on the use of technology to provide a better service to the customers and to improve our own profitability.

A word about my role at Wells Fargo and our philosophy on strategy and technology I think might be useful in helping to establish a base line from which I can then talk to you upon—talk with you on some of these issues of telecommunications and security.

About 3½ years ago the senior management of Wells Fargo did an introspective review of itself. And the management drew—

looked at, I might say—and I put this in context of 3½ or 4 years ago, some of the conclusions that were drawn are obvious today. They were less so 3½ or 4 years ago.

But we looked at the time at the Wells Fargo—the environment, the probable bank regulatory environment years hence, looked at technology and its future direction, drew several conclusions which I think bear on this issue—some indirectly, some much more directly—on security.

The first was—now obvious, then not so—that banking would undergo a tremendous change in the way we dealt with issues of banking. Those changes would be rapid and very dramatic. Successful banks would be those which understood the use of technology, which understood technology and how to use it, that the effective employment of technology would create great opportunities but with it would be—with those opportunities would be problems which would appear to be intractable as we proceeded but problems which would have to be confronted very decisively.

And we saw security as being one of those problems, data security, information security, as being a problem which would appear to be—have many intractable attributes but would have to be confronted decisively.

We felt that the concept of planning, business planning at the corporate level, followed by ad hoc technology initiatives supporting that business plan would not serve us well in the future.

And finally, we felt that in order to manage banking in the future effectively, and Wells Fargo specifically, would require very strong financial controls, very concise and useful management information, and finally strong standards and procedures, particularly as related to computer operations and security.

Following those conclusions, the senior management created the position which I now have at the bank, or at the company, where we combined business planning or strategy with technology planning and strategy to include security and personnel.

We believe that a bank has only three assets basically. It has its capital, it has its information, and it has people. And each of those three assets have to be protected equally, so that we have put under one office the responsibility for dealing with the capital or the assets, the capital assets, embodied in a business strategy, information or technology, and finally—and security, and finally people, or personnel.

At this point I would like to make an assertion that I think is probably very important. It has probably been made to you by—by most every speaker that has been here, witnesses been with you, and those that will come subsequently.

But the two authors, Bill Sinnett and Bill Gruber, in a book called "Information Resource Management," make the statement that telecommunications is an enabler. It's an enabling technology rather than a technology with an end in itself.

So when one deals with telecommunications without dealing with the supporting computers and terminals—and this applies, of course, to security as well—he is dealing only with an enabling technology and missing the point.

So that as I—I think one can only deal with telecommunications security by dealing with security, and based on that, in my subsequent comments, I am—when I speak of information security, I am speaking of telecommunications as well as computer and personnel and all of the terminal, all of the related aspects.

At Wells Fargo—and I will take just a moment on this—at Wells Fargo we have a very large and complex computer communication structure, which I think is typical of the large banks. As with other banks, all of our systems used to be essentially badge processing. With badge processing, the security issues are principally physical, but as the technology evolved and we began to offer new products and services, we found that those products and services and the management of the bank itself could be facilitated on a day-to-day basis by online capabilities.

As online capabilities or the so-called online era came to be, we increased the number of terminals, we increased the access which employees had to those terminals, and then again, as the technology proceeded, we increased the number of customers that would have access to these same terminals, so that we have moved from an era in which we could secure our information assets by walls and locked doors to one in which we are spread worldwide with large numbers of terminals online to multiple computers and online to customers, as well as bank employees, so that the issue, for example, of dealing with trustworthiness of your own employees becomes one of—one of—one issue, but it's also dealing with customer sets and other vendors and other companies because our computers in the banking industry are connected not only—that is, our terminals are connected not only to our own computers, but our computers are connected to other computers, so that we are dealing with an issue that is broader than simply dealing with the trustworthiness of your own employee.

And finally, the terminals themselves as technology progressed, the terminals were given intelligence so that terminals themselves became computers and then we have added to that the so-called personal computers, which adds a dimension of complexity which probably exceeds that with which we have had to deal previously.

In summary, then, there has been an evolution that's occurred in our processing that has created for us—moved us from an area in which we could seal through doors, locked doors and walls, to one that we have to deal—we have to seal through some sort of electronic keys. It's obvious that—that the security issues then have become extremely complex for us.

Now, in general I think the Department of Defense and related intelligence activities have understood security and it's been a way of life, if you will, in the Defense Department for some years. Other of the Federal agencies, I think—and I am not speaking as an informed individual on this—but other agencies have come more recently into understanding security issues.

The private sector—and here I speak of the nondefense private sector—has been much slower in understanding the computer exposures, the security exposures which they have. I think management in general has early on—took the position that in order to secure electronic—provide electronic security was so expensive that it would take funding of the—of the—of the manner of the National Security Agency in order to provide the kind of security, and that was beyond the company's means, and I am not speaking here of

Wells Fargo, but in general, that it was best just to hope that nothing ever happened and the security was just too expensive.

Management I think in general has been better served in the last 5, 6, 7 years by realizing there—there is a great deal that can be done in information security in the private sector by realism, by the proper use of technology, by being realistic, by the proper use of technology, and by limited though not insignificant funding, so that management in general in the United States I think, private sector, has taking a much more realistic attitude and understands the vulnerabilities though, as I think as Dr. Ware said, it probably is spotty across industry. Certainly the banking industry has, I think, led in dealing with security issues because there has been an understanding.

I would like for just a moment to talk about the Wells Fargo security program. Again, I think it's typical of banking, but I speak only, of course, for Wells Fargo.

Our security program starts with the assumption that security requires a specific corporate attitude, and that corporate attitude must exist from the very senior people downward with four tenets or principles upon which it is based.

One is that information security has to be understood throughout the bank by all employees. We believe that security is not a project but it's a way of life. We believe that it is everyone's responsibility. Third, that our security program is designed to prevent losses, not to catch someone doing something wrong. We think, finally, that potential losses and losses, potential exposures, need to be reported very quickly so that one is able to reduce the exposure and to understand why it did occur and to take appropriate actions.

Now, those are the four principles. They might seem apparent to you, and I think in the defense establishment they are apparent. They are not so much so I think in the private sector. And I might point out that the four principles that I just mentioned to you would serve well as a national set of principles dealing with security in the nondefense sector.

We then think—we—we take the—a number of measures, specifically technically measures, within the bank and Wells Fargo & Co. to secure our data, and I won't go into them. They are typical conventional procedures such as password control, such as if a person fails with his password attempt either on two, depending on the system, either are two or three tries. He is disconnected and his password is locked out.

We use encryption, where it is cost effective to do so, both data encryption and bulk encryption where it is cost effective. We have a security program, a set of policies which have been written, to govern everyone's responsibility Wells Fargo & Co. for security.

So, I think our program is good. We have a number of areas, however, that are beyond our control and beyond the control of the private sector that I would like to discuss just briefly with you, pointing out that I think none of these are original, they certainly are not profound, but they are areas in which I think the Federal Government can provide assistance.

One of them—one of them deals with a very broad social issue in the United States, and Don Parker from SRI has stressed this before. I don't know that he did when he talked with you. I think he did speak with you. But—and that is the fact that we are teaching individuals, particularly young people, the use of computers in the elementary and the high schools and college level. We are encouraging them to be as innovative as possible with the use of personal computer—with the use of computers and terminals.

We are at the college level even challenging them to break systems, but at the same time, we have failed to provide a basic set of ethics and moral tenets around which their activities ought to evolve.

Now, you would say we know—we know from home and school that it's wrong to break into a bank or break into a bank, so why isn't the same true of a computer? Well, the fact is we encourage them to use the computer in such ways that they will break into—into data bases and other computers.

We have almost created an environment which says it's all right to break into a computer. As long as you don't steal anything, as long as you don't destroy anything, it's OK to see if you can do it. And my suggestion to you is that—and I am not suggesting there should be a law that mandates this—but that we need to create an environment in the public schools—in the schools in which there is a code of ethics and morals taught at the same time we are teaching a very powerful technology to students.

The second problem I think is one of a great lack of understanding and knowledge on the part of the private sector and the public on security. Now, while I would support, for example, the need for a handbook—and I would suggest that such handbooks do exist—there are a lot of unknowns in the area of security. We can tell people how to operate a computer center—and we should, people should know, people who operate them should know—but the fact is that we have very big potential exposures in detailed areas about which we know very little in the private sector.

If we had unlimited funds and we could have encryption, for example, that's approved at the national security level, that would be one thing, but we can't afford that. So that we have loopholes and gates and entry points into a lot of the software, for example, that we don't know about, and the private sector is unaware of many of these and can't be aware of them.

It's for this reason that I would support and urge two aspects which have been discussed with you previously. One of them is the creation of a national commission, but I would caution that if that commission is created and approaches the problem from the national security standpoint alone and deals with very high-level issues of defense and National Security Agency and defense-related industry it will be, in the long term, less effective than if it is able to deal with the pure commercial private sector problems and the public awareness areas, about which nothing has been done, to my knowledge, in the past.

The second initiative along this line, the same that has—that has been mentioned by—by others is the creation of a—of a group, research and development institute of some sort to begin to look at very real and what I would say to the defense sector very real but mundane and pedestrian issues dealing with security, a research institute. Now, I wouldn't suggest that it be a national institute, but I would suggest that it would need to have—it would be desirable for it to have congressional support.

A third area that I think is important, and that is, it's obvious to us all that the Federal law enforcement agencies, the Secret Service, the FBI, the Federal prosecutorial staff, are heavily involved with computer crime. It is our sense, however, that these activities may not be funded at the level necessary to permit those agencies to do the job that they are chartered to do.

A recommendation here is fairly simple. It is that the legislative and executive branches be cognizant—appropriate agencies be cognizant of the need to improve information security in the private sector and to insure that there is appropriate funding for agencies such as the Secret Service—excuse me, the Secret Service, the FBI, and the prosecutorial staffs.

In a related manner, I am aware that the Federal agencies—the FBI, Secret Service—have very elaborate, very effective training programs for their own individuals. I would think that much of that material, either through closed circuit TV or video film or training materials, could be made available to the private sector.

I would also suggest that, going back to what I had said earlier about a lack of understanding on the part of the private—many of the—much of the private sector on security issues is that some sort of certification procedure be established to permit or—that is, to permit private sector firms, technology firms, to submit techniques, equipment, for example, software, for certification, not requiring activities, not requiring a bank, for example, to install certain equipment, but certifying that that equipment in fact meets the specifications which the vendor has, which he has himself established.

Finally, there is current legislation pending. We support that legislation for several reasons, not, incidentally, because we believe that without the current legislation that's pending one cannot prosecute trespassers because in the main I think, even with existing legislation, crimes can be prosecuted.

But we would support it for three other reasons. One is that the prosecution would be facilitated; second, it would heighten public awareness; third, it would serve as an obvious deterrent at least to the less hardened criminals; and fourth, and I think very important and maybe overlooked, and that is the fact that the United States did not lead with privacy legislation, lead other industrial countries, and so that Europe principally, Canada, established, adopted privacy legislation which led and caused problems in transporter data flow, for example, which we might have avoided had we been first in the legislation.

So that I would urge that legislation, if passed now, could serve as a guideline to the other industrialized countries so that we don't find ourselves being defensive on measures that we need to take. And this I think we can go back and look at the history of transporter data flow and its problem to see that there is a very real possibility that other countries will get legislation before we and we will be driven in ways that we don't like.

Mr. Chairman, I have appreciated the opportunity to be with you and will answer any questions that you might have.

[The prepared statement of Mr. Hancock follows:]

PREPARED STATEMENT OF JACK L. HANCOCK

Mr. Chairman, I am Jack L. Hancock, Senior Vice President of Wells Fargo & Company. I am responsible for a function at Wells Fargo called Strategy and Systems. I will elaborate on that in a moment. I am happy to have the opportunity to be with you today and offer my views on the very important topic which is the subject of your hearings. Wells Fargo & Company is the parent of Wells Fargo Bank. Both are headquartered in San Francisco, California. The bank is the 12th largest in the United States in terms of assets ($25 billion), and is the oldest in California. We are a bank which has placed heavy emphasis on the use of technology to provide better service to our customers and to improve our profitability.

A word about my role at Wells Fargo and our philosophy on strategy and technology may be useful in establishing a base line from which I can talk in more detail about telecommunications security. Approximately 3½ years ago, the senior management of Wells Fargo & Company examined the current financial industry and its probable future, the economic environment, Wells Fargo's structure and competitive position, and our employment of electronic technology and the future direction of that technology. Senior management drew several conclusions, some of which are very obvious today, but were not so obvious at the time:

- The banking industry would go through a tremendous change in the coming years.
- Those changes would be rapid and dramatic.
- The successful banks would be those which understood technology and how to employ it effectively.
- The effective employment of technology would create great opportunities, but those opportunities would be accompanied by problems, some of which would appear to be intractable, but which would have to be confronted decisively. We saw information security as being among the most difficult.
- The traditional concept of doing business planning at the corporate level, and following that, with ad hoc technology initiatives supporting the business plan would not serve us well in the future.
- To confront the future effectively would require strong financial controls; concise, useful, and timely management information; and strong central standards and procedures, particularly as they relate to communications and computer operations and security. These central requirements became more important when our management concluded that a large bank such as Wells Fargo could move decisively only if the business decisions were decentralized to the line groups.

Following from the conclusions described above, we created a small group that reports to the Chairman of Wells Fargo & Company. We combined the responsibility for developing our business strategy and associated technology strategy to include all aspects of security. Planning, per se, is delegated to the line groups which do their planning under the strategy umbrella (business and technology) developed for the company.

We believe that a bank basically has only three assets; capital, information and people. All three of these components must be understood, managed and protected equally well. Therefore, the human resources for personnel function is also assigned to strategy and technology. Thus, from a single point, we are able to look at and deal with safeguarding, from a corporate perspective, our three assets: capital, as represented by our business strategy, our information, and our people.

Let me, at this juncture, make a point which I suspect has been made by many of the individuals who have appeared before you thus far and who will appear before you subsequently. Authors Bill Synett and Bill Gruber, in a book called Information Resources Management, state that telecommunications is an "enabler", that is, telecommunications is an enabling technology, not an originator or processor of information in the strictest sense. Thus, telecommunications enables organizations to integrate computers, business applications, office systems and business processes into a coherent and very powerful whole. For this reason, one cannot consider the subject of telecommunications security and privacy without linking it to computer and systems security as well. The fact is that when a user of a system, whether that user is a customer or an employee, uses at a terminal, he is most typically accessing applications and data bases contained within and processed by one or more computers tied together with his terminal through communications. If there are security deficiencies, they may be in the communications links, but more frequently, they are either in the terminals or the computers. Thus, as I speak with you about data and information security, it will be in the context of combined computer/communications.

At Wells Fargo, we have a very large and complex computer/communications structure which is typical of major banking institutions. As with other banks, our systems used to be essentially batch processing. Thus, security was basically physical in nature. As technology evolved, we began to offer new products and services, and found it desirable to manage these products on a day-to-day basis through on-line capability. With the outset of this "on-line era", the number of terminals, as well as the number of users increased. These users were almost always employees of the company. However, over time, the number of on-line terminals increased, and employee users increased, and we began to provide terminal service to customers as well. At the beginning of the on-line era, data resided in a single computer and the link between terminals and the computer was simple. However, technology made it possible to spread data among computers, further complicating the system. The terminals which we used originally had very limited functional capability, that is, they were "dumb" terminals. Again, technology progressed so that a processing capability was added to the terminals and the terminals themselves became computers or "intelligent terminals" as they are called. Finally, the advent of personal computers added a dimension which surpasses in complexity, that with which we have had to deal previously.

In summary then, an evolution (some would call it a revolution) has occurred in the information processing arena and we found ourselves moving rather quickly from an environment which we could seal by walls and locked doors to one which extends literally all over the world through communications, with the input and output being provided by many on-line terminals, themselves having processing capability, and being operated not only by bank personnel, but also by customers and individuals serving the bank through many different capacities (vendors, communication firms, outside processors and the like).

It should be obvious that as this rapidly changing technology developed and was implemented, security has become increasingly important, and the provisions of that security increasingly complex.

In general, the need for information security has been well understood for many years in the defense and related intelligence activities. The need for information security began to be accepted in the non-defense governmental entities much later. In the latter case, the requirement was given special emphasis by legislation enacted in the mid and late seventies. However, the private sector was much slower to respond to security requirements. There are probably many reasons for this, but one would seem to have been the belief on the part of senior management that the problem of information security was so big that it could only be solved by massive expenditure of funds in the manner of the National Security Agency. As the funds were not available at that level, there was the simple hope that "nothing untoward would ever happen". My sense is that in the past few years, this has changed and management has been better served by the realization that there are many measures that can be taken, using current technology, realism and reasonable funding, to begin to solve their information security problems. There are, of course, limitations with the current security technology and we need to address them.

I would like at this point to discuss with you a few key elements of our security program at Wells Fargo. I believe that what we are doing is enlightened, but I also believe it is very typical of large banks. Of course, availability of security technology and costs still limit our ability to deal effectively with the entire potential exposure that we have.

Our security program starts with the assumption that the right information security program involves a specific corporate attitude. We believe that information security is not a project, but is an ongoing and integral part of the day-to-day functioning of the bank. Our program is based on four tenets:

- Our information security program must be understood throughout the bank.

- Security is everyone's responsibility from the most senior executive downward.

- Security is designed to prevent losses and not to "catch someone" doing something wrong.

- Losses, or potential loses, must be reported accurately and promptly so that corrective action can be taken.

The requirement of the first tenet would seem to be apparent. However, it is less so in the private sector than one might think. For the most part, private sector companies, except those dealing with national security, have not until recently had any formal way to measure and designate the sensitivity of information which the organization possesses. That is essential to an effective awareness program. It is equally essential that all employees believe that the information with which they work needs to be protected from loss. We have a program for reviewing all information systems and the data within them and categorizing each by level of sensitivity. We have spent much time and company resources emphasizing this and trying to make information security a way of life without excessively restricting access to information when it is required.

The other tenets follow from the first. We have made responsibility for security the requirement of every employee of the bank and we have in place a reporting structure which makes knowledge of security lapse evident fairly quickly.

The four tenets on which are program is based might well represent the ideal national program for information security in the private sector.

On the technical side, we follow conventional security procedures such as the assignment and implementation of passwords and other access methods to on-line systems. We are using encryption where it is cost-effective and we subject every system to rather rigorous design and development rules and to multiple post-implementation audits and examinations.
Thus, it is our feeling that we are taking appropriate and cost-effective measures to protect our information.

There are, however, shortcomings which exist in information security which are largely beyond our control and in which we believe the Federal Government can provide assistance.

One of these revolves around a national social issue. Specifically, as Mr. Don Parker of SRI has stressed, and we agree with him, attempting to enter or entering a computer system without proper authorization is wrong. Teaching individuals, particularly young students how to use computers, without teaching them the ethical and moral aspects of computer technology, is leading to an unfortunate national attitude. It seems as though there is a feeling that attempting unauthorized access to a computer system is fun and games, particularly if nothing is lost or stolen. This attitude needs to be changed and schools that teach computer science must also teach the ethics and morals associated with computer use. Otherwise, we will have a very serious crime problem in the future.

A second problem is that there is great lack of knowledge and understanding of the scope of information security problems and their various solutions. In part, there is a lack of awareness, but in larger part information security is simply not understood. We need greater knowledge of the threats and potential risks, and public awareness needs to be heightened. We suggest that this can be done by the creation of a panel or commission to assess our information security vulnerability in the non-defense area. This should be a high level group whose members have national credibility. The panel members should have a business and not a technical orientation, although, of course, they should be provided with technical support. The idea of a blue ribbon security panel is not new, but it is one that has not been implemented and which we believe could go far in helping all of us understand the exposures and deal with them.

Third, it is obvious that the Federal law enforcement agencies, such as the Secret Service, the FBI, and the Federal prosecutorial staff are deeply involved in dealing with crimes related to computers. It is our sense, however, that these activities may simply not be funded at the level necessary for them to provide the coverage and assistance necessary to meet their full responsibilities. Our recommendation in this connection is simple. It is that the executive and legislative branches be fully cognizant of the need to improve information security in the private sector and insure adequate levels of funding for the appropriate agencies.

In a related manner, we are aware that the Federal agencies such as the Secret Service and the FBI have excellent training programs designed to help their agents detect and investigate computer crime. We would suggest that consideration be given to systematically expanding those programs to permit participation by private sector firms such as banks. This could be accomplished fairly simply by making available appropriate programs through close-circuit television or videofilm. Sharing of appropriate textual material should also be considered.

Fifth, there are many new initiatives in computer security devices and techniques. Every week seems to bring a new one to the market. However, it is virtually impossible for a single private organization or even a grouping of organizations to research these, assess their effectiveness, and integrate their implementation effectively.

Therefore, in this connection, there is a need for assistance to the private sector at two levels:

- o A certification procedure by an independent agency certifying that a device or technique meets specified minimum requirements. Private sector companies should be free to acquire or implement such devices and techniques as they desire, but the certifying process would give them confidence that they are getting the capability specified by the vendor. This is a very complex area and would have to be carefully studied, however, it would seem to have merit.

- o Mr. Robert Campbell, a well-known computer security consultant, has suggested that there is a need for an independent, privately-supported facility to provide computer security research for the private sector. We support the creation of such an institution, but believe that its success will depend on full support of the Congress and the Executive department.

Finally, current computer crime legislation which is now pending at the Federal level, should be enacted to better define computer crimes. We support the legislation not because we believe that most computer crimes cannot be successfully prosecuted today -- most can be; but because:

- their prosecution would be facilitated
- the publics awareness would be heightened
- it would serve as an obvious and potential deterrent to the commission of computer crimes
- finally, and probably not well understood, passage of Federal computer crime legislation would serve as a pace setter or guide for other industrialized countries. You may remember that several other industrialized countries moved decided ahead of the United States in the area of privacy legislation and the transport of same across borders. They thereby set standards which have resulted in difficulties for the United States in transborder data flow. The Congress has the opportunity to gain for the United States international leadership in computer crime legislation and avoid the problems which occurred with transborder data flow.

In summary, banks are actively pursuing information security programs which are effective. However, there are a number of steps which must be taken to improve these programs. We are doing our part, but believe that there are several positive steps which the Congress and the Executive branch of the Federal Government can take to facilitate this effort.

I appreciate the opportunity to meet with you. I am prepared to answer any questions you may have.

Mr. GLICKMAN. Thank you.

Mr. McCandless, why don't you begin the questioning?

Mr. McCANDLESS. Thank you, Mr. Chairman.

Mr.—General—Jack, during our respective times in the service we have seen the scrambling and unscrambling of messages at each end over broad expanses of water, terrain. And with respect to then sensitive information of a nongovernmental nature but a business-type nature, where inventories or whatever it might be, the cost of a commodity would be of importance to your competitor, is that—did I understand you to say that that is a prohibitive part of the hardware involved?

Mr. HANCOCK. We are doing that on selected—in selected areas, but it is a—it's costly and there are some very real problems with managing—with managing this encryption or scrambling because within the Defense Department one is able to manage it since both ends belong to the Defense Department or both ends belong to Government agencies, whereas in the private sector, one end of a circuit may belong to the Federal Reserve and the other end belongs to Wells Fargo Bank, one end may belong to another bank, to another company, and so that we get into problems of managing the keys and—which itself is a problem, and then the cost is very high, and we believe that technology is available to reduce that cost. And that is the sort of thing that I would like to see research effort devoted to. We don't need security devices at the level of the Defense Department, but we do need security devices that will provide a reasonable level of security.

Mr. McCANDLESS. Your other comment about the fact that security needs to be a corporate attitude, not a project but a way of life, is that a part of the indoctrination of your basic employees when they enter your system?

Mr. HANCOCK. It is, and that's exactly, in the last 3 or 4 years, what we have started to do as a part of the overall policy. People, when they come in, sign statements that they understand that, and we've stressed, it and it is at all levels.

Mr McCandless. To what extent do you go with an entry level teller, for example? I will use that as an example.

Mr. Hancock. Well, we have entry orientation training programs so that from the very—and a teller is a good example because we have special teller-training programs, and security and privacy are topics which are discussed during that initial training, and then during the programs—during their day—daily work, it is a matter that is stressed with them by supervisors.

You would ask, I think—if you would ask our tellers, you would get a fairly, I think, good response from them that they understand it. Of course, we are like any other organization that is fairly large, and it is naturally at times spotty, but it is a matter that we have tried to—we have another program called Managing the Wells Fargo Way that includes security as a—as a topic that is taught in the programs.

Mr. McCandless. Without getting big brother Government involved to the degree that they are calling the shots, what would you say to us as this committee would be your recommendation as to the highest priority in this field that—that we should move on, we meaning the governmental process?

Mr. Hancock. I think the idea—I think there are two. One is the legislation that is pending, but second is the creation of a commission.

Mr. Glickman. Do you mean the computer-crime legislation that is pending?

Mr. Hancock. Yes, and second is the panel, the creation of a commission or a group that is fairly high level to start—to really look at the indepth—the problems.

Mr. McCandless. Thank you, Mr. Hancock.

Thank you, Mr. Chairman.

Mr. Glickman. Mr. Hancock, just curiously, we have encountered some reluctance by the private sector to testify about the problems in computer-communications security. To be honest with you, your organization was one of the few that volunteered, and some that we had pressed very hard, some that have daily contact with millions and millions and millions of people and whose evidences of ownership are found in most billfolds in America, did not indicate a very strong desire to testify.

Why? Why do you think that is the case?

Mr. Hancock. Well, I'll not presume, obviously, to speak for anyone other than myself or any company other than Wells Fargo. But I would suggest—first, I will preface my comments in telling you that it was not without some considerable thought that we agreed to, that we thought—that we volunteered, if you will.

We did so because we think that this is a terribly important subject and one that is of large national concern, or not concern, but large national importance. I think, probably, the reticence comes about for two reasons. One is that in the short term it's not clear that an organization like Wells Fargo in the short term that we will benefit from this.

There is—it's not—I certainly don't think it's like the individual that watches a crime being committed on the street and then is reticent to get involved. I don't think it is that at all. But I do think in the short term, one opens himself to the possibility of people taking shots at you. That is a very real short-term, practical problem that concerns—that would probably concern anyone.

Second, certainly not the banking industry, but there are other industries that you might have invited that are probably ill-prepared to discuss the subject and have not done very much.

We think we've got—we know we have deficiencies in the bank—in Wells Fargo in the banking industry, but at least to think, we are aware of those. And I think many of the kinds of industries you might have elicited or asked to participate simply may not have felt competent to talk about very much, and that deals with why we need, I think, heightened awareness on the part of the public and the private sector.

Mr. GLICKMAN. Yes, I think both reasons are valid reasons for not wanting to testify, although I think the second one is more valid than the first one.

Let me ask you this. You've indicated that you in a sense have installed some of the mechanisms, that Mr. Ware referred to, to prevent unauthorized access. To your knowledge, have most banks in the country done the same thing, most major banks in the country?

Mr. HANCOCK. All that I know of that have, I think—I would doubt that you would find any major bank that has not gone through fairly rigorous installation of procedures, password control, special software. The big banks, I know, are very much aware of it.

Mr. GLICKMAN. And in terms of the current state of the problem and the current technology, you think—would you agree with Mr. Ware that currently the technology is available for you to protect the assets of your bank and the privacy of your customers? I am not talking about what's going to happen in the next 10 or 20 years but right now, if properly used and managed, that technology is acceptable?

Mr. HANCOCK. I think it is. The technology, much of it is probably too expensive, much more expensive than we would like. We spend, Wells Fargo, in excess of $11 or $12 million a year on security, which is, comparatively speaking, a lot of money. It is—depending on how you look at it, it's about 1.3 percent of our noninterest expense, so it is not a small amount of money.

Mr. GLICKMAN. Do your insurance carriers require you to provide some of the security?

Mr. HANCOCK. Your question or the one that—one of you asked that question earlier. Insurance carriers are very much aware of this now, and we have, at the request of our carriers, have gone through security audits, for example, to help them understand that we are taking prudent measures.

So that in the insurance industry, vis-a-vis the banking, that as its customers the insurance is doing a lot in this area, and I think we are going to see more of it as the insurance industry realizes that it can minimize its own risk and the banks reduce their premiums by insuring that we have—by seeing that we have taken prudent measures.

Mr. GLICKMAN. Yes. A depositor at the Wells Fargo bank, should he feel secure that his deposits are protected in terms of privacy as well as from manipulation by outside parties?

Mr. HANCOCK. As far as manipulation, he should feel absolutely secure because we—it is our obligation. We are obligated to him, and he will not lose money. With respect to the privacy, the answer is yes, also. And I say that because we've taken what we consider to be every possible step to protect his privacy, but there, of course, privacy, unlike money, if an individual loses a deposit with us, for whatever reason, we can make that up. If you lose information, once it's exposed, it's exposed.

Mr. GLICKMAN. It used to be that I could call up a bank on the telephone and ask, "What is my account status? How much is in the account?" If a customer calls the Wells Fargo bank—it can't do that by telephone anymore?

Mr. HANCOCK. No, except—except we have some arrangements with corporations, of course, where we have an authentication system with them and with a customer where an account number and some other personal information can be—can be used. But the answer to your question is no, as a matter of policy.

Mr. GLICKMAN. OK. As you expand your information systems capability, what new dangers do you see as being a major problem; for example, banking in the home or different methods of communicating with the bank, electronic mail with your bank?

Mr. HANCOCK. Let me also differ a bit with Dr. Ware in answering the question. I do so not because I don't agree that electronic mail and security for electronic mail is no different than security for other online systems, but customers want—and understandably so. We all want it both ways. We want to have secure systems, we want to have security of our information, but we don't want to have to go through any sort of hassling when we want information. When you call and want your balance, you want your balance, and you don't want to be—you don't want to be told you can't have it.

So, we see one of the problems is the public awareness, that when we exercise prudence—we, the bank—exercise prudence with your account, that we are doing it for your good and this is an issue of public awareness.

We, for example—corporations understand, large corporations that are transferring large amounts of money, the Federal Reserve, for example, understand the need for authentication systems, and they are not reticent if they cannot give us the right authentications. They understand why we are not going to move the money.

But customers are not always that way. So when we get into home banking, I can see areas that not only will there be technology areas, but there is going to be customer acceptance, a willingness on the part of the customer.

When a customer uses one of our ATM's, for example, and gets three tries and misses his number and the machine takes his card, he is not happy, even though he understood that he forgot his number. And you can have these lapses. We have all done it. So I think part of the problem is public awareness and the need to heighten that awareness and the fact that security is a public issue, not just a bank issue.

And then there are—you visualize a communications network today with a large bank that, as I said earlier, consists of multiple computers tied together in that computer set within your own bank and then these, in turn, tied to brokers and tied to computers by the Fed and the clear—New York clearinghouse and the California clearinghouse and then on terminals and intelligence terminals. One just gets in an enormous maze, and that again speaks to this—this lack of knowledge.

I can tell you, as many people can, I can explain to you how you secure and how you deal with this and the question earlier about we have always had locks on filing cabinets. But we have understood those locks and the lock was only one place and why don't we keep the key in our pocket. But electronically it is so complex that we have very real problems in understanding even where our exposures are.

Mr. GLICKMAN. Just briefly, two additional questions. Do you use tiger teams to test your own security?

Mr. HANCOCK. We do. We do. Two groups. One is our internal auditors and the second is a small group of people who are matrixed to me who spend their time seeing what exposures and how they can get to our systems.

Mr. GLICKMAN. And you would recommend that for any major corporate user of computers?

Mr. HANCOCK. I think it's essential.

Mr. GLICKMAN. Have you had any interreactions with Government agencies in setting up security systems? I mean, obviously from your past experience you have but I mean since you went in this job?

Mr. HANCOCK. At two levels. One is with the Federal Reserve, which is very well aware of the problems. And the second, the Treasury Department has recently had a number of initiatives that are leading to an exchange of information between the Treasury, ourselves, banks, and law enforcement agencies. I would commend, in fact, Treasury at this level for much of what's happened recently. Been very effective.

Mr. GLICKMAN. Yeah. Their testimony was excellent to us. They seemed to be far ahead of any other Government agency.

Mr. HANCOCK. I think so.

Mr. GLICKMAN. Thank you very much, Mr. Hancock. We appreciate your excellent testimony.

Mr. HANCOCK. Thank you.

Mr. GLICKMAN. Our next witness today is Mr. Julius Cohen, director of technology, Grumman Aerospace Corp.

Mr. Cohen, it is a pleasure to have you here today.

STATEMENT OF JULIUS COHEN, DIRECTOR OF TECHNOLOGY, INFORMATION RESOURCE MANAGEMENT DEPARTMENT, GRUMMAN AEROSPACE CORP.

Mr. COHEN. Mr. Chairman, I am pleased to testify before your subcommittee on telecommunications, security, and privacy.

To begin with, My name is Julius Cohen. I am technical director of the information resource management department of Grumman Aerospace. I will present some of the problems associated with computer and communication network security as they affect their manufacturing company and, in general, Grumman.

Our corporate headquarters is located at Bethpage, Long Island, where we have our engineering capability, our manufacturing facilities, and data processing. In addition to this, we have other locations on Long Island, as well as in the States of California, Florida, Georgia, Maryland, and Texas.

Our primary products are for the U.S. Government, and in particular we are a major supplier of carrier-based Navy aircraft systems. Since military security is strictly defined by the Department of Defense, we are well-disciplined and oriented towards security.

Our facilities are completely enclosed in a chain link fence and access is controlled. Employees must show a picture badge on entry, and visitors are escorted and only have limited areas that they can access.

Our physical security, as well as the extraordinary precautions required to safeguard classified information, has made us feel, at least in the past, that all valuable information was protected. This environment, which emphasized the need to protect classified military data, indirectly created an incorrect impression that information not classified was not valuable.

Over the past few years we found out that a lot of our information is of value, and the two in particular are that of private data—this includes medical records, payroll information, and employee information—as well as proprietary data. This is data which affects us in the competitive field that has to do with our business plans, our manufacturing capability, our financial data.

Mr. GLICKMAN. Why don't you move a little closer to the mike and make sure the light is on there, so we can hear you.

Mr. COHEN. All right. Is this better?

Mr. GLICKMAN. Much better.

Mr. COHEN. OK. I am sorry.

I will not discuss here today classified data as defined by the Department of Defense, but we will discuss security information as it affects our proprietary data and our private data.

Since Grumman operates in a multi-State environment—and that is, we have plants all over—we have a large interconnected telecommunications system for both voice and data. With the advent of rising costs in telephone and the divestiture of AT&T, the company reexamined its use of telecommunications and came up with a new plan whereby we plan to institute our own telephone company. In fact, we are in the process now of building a terrestrial microwave link on Long Island to connect all our plants, and in the near future we plan to use satellite communications to the various States.

For a long time everybody considered telecommunications as safe. Wire tapping was a physical thing. It was against the law. A perpetrator had to get to some type of physical access. However, long distance telephone communication today is by microwave or satellite. This means that you need no physical access other than to have equipment which can receive the radio waves, record them, and then later analyze them. On this basis everyone must assume that any data or voice communication that goes long distance is being monitored by someone.

Grumman has reached the position also where the computer is an integral part of its everyday operation. This has to do with the normal business affairs of payroll, inventory, accounts receivable, as well as our ability to design and build products.

We have an extensive CADCAM system. In this area, our engineers sit at a terminal. They literally design the part on the scope. This is transmitted to manufacturing, where quality control inspects the product. Tools are made from the data, and machines actually cut parts. As a result of this, we have to be sure that none of this is interrupted by anyone.

There are many computer—there are many computer networks within the company. There is our CADCAM systems, there are our large IBM data bases that run the business aspect, there are small minis and micros that run software development, and recently we have even purchased a supercomputer, or Cray, for our engineering and research work.

In addition to that, several years ago there was an unsuccessful attempt to break into our systems. Here a local high school student, with his home computer, using his telephone, called Washington, D.C. and through Telenet gained entrance at least to the system.

As he tried to log on unsuccessfully, one of the system analysts looking at the data wondered why somebody was continuously trying to log on and not succeeding. On calling the FBI and working with them, we were able to apprehend the intruder.

As a result of all of this, we realized that security was a balancing act of where to make the terminal and the computer accessible to the user, we also had to do something to protect the data and the information. As a result of this, we put out several years ago our corporate directives. This was to tell people what they must do and why as far as security and, equally important, what they must not do.

We defined in these directives both private data and proprietary data, and we made the rule that any private or proprietary data that went out on the telecommunications network had to use encryption devices which conformed to the National Bureau of Standards data encryption standard and the Federal standard 1027 endorsed by the National Security Agency.

By the way, I would like to say that we did work with NSA's Communication Protection Special Projects Office, and they were very helpful to us, both in setting up the directives and in selecting the equipment to work with.

One other point or one other problem we face, and that is the microcomputer. It is a very, very, versatile tool. It allows somebody to take a lot of material very quickly, analyze it, and use it. It also is a method of transporting a lot of data very easily on a floppy disk.

One of the things we are trying to do is incorporate the use of this piece of equipment into our networks without compromising the security of the network. To date, this problem is very serious. We really do not have an answer on it now, and we are working with various agencies to attempt to get that answer.

One other thing we have done, and that is, once you have accessed the computers, there is software within the computer that limits where in the computer and what data you as a user can go to.

We have put in a commercially available piece of software called ACF2. This keeps an audit trail of everyone who comes into the computer and where they go. It limits the data that a user may get and may not get. It keeps a record of attempts of people to get data which they are not authorized to do and, in general, is a precaution on our systems. I might point out that we do use cyber machines in our scientific area, and that this software is built into their normal operating system.

The cost of security has been discussed previously. It is not trivial. In the next year or so we spent—we plan to spend over $1 million in hardware alone for encryption devices in order to protect our data as it goes out on the telecommunication lines. In addition to this, we plan to spend additional money in the form of people to put up software packages for protection of the data within the system.

We believe we are doing a good job. However, we are not complacent. We realize that the better we get, the better the intruder gets and, therefore, it is a common fight to see who can win the battle.

Thank you.

[The prepared statement of Mr. Cohen follows:]

TESTIMONY OF MR. JULIUS COHEN
BEFORE THE HOUSE
SUBCOMMITTEE ON TRANSPORTATION,
AVIATION AND MATERIAL OF
THE COMMITTEE ON SCIENCE
AND TECHNOLOGY
OCTOBER 24, 1983
RAYBURN HOUSE OFFICE BUILDING - ROOM 2318

Mr. Chairman, I am pleased to testify before your subcommittee on telecommunications security and privacy.

My name is Julius Cohen. I am Technical Director of the Information Resource Management Department, Grumman Aerospace Corporation (Grumman). I will present some of the problems associated with computer and communications network security as it effects a manufacturing company in general, and in particular, Grumman.

Grumman's corporate headquarters, engineering capability, manufacturing facilities and data processing center are located in Bethpage, New York (See Figure 1). Grumman has additional facilities at other Long Island locations as well as in the states of California, Florida, Georgia, Maryland, Michigan and Texas (See Figure 2).

GAC primarily manufactures products for the United States Government and is a major supplier of carrier based Navy aircraft systems. Since military security is strictly defined by The Department of Defense, Grumman is well oriented to and disciplined in military security matters. Our facilities are completely enclosed by a chain link fence with controlled access. Employees are permitted entrance only by the display of a picture badge; visitors are escorted and only have limited access. Our physical security as well as the extraordinary procedures required to safeguard classified information has made us feel, "at least in the past, that all our valuable information was protected".

This environment, which emphasized the need to protect classified military data, indirectly created an incorrect impression that information not classified was not valuable.

Over the past few years, concomitant with the rapid expansion in the use of computers, we recognized that unclassified information is also valuable. For example, there is information of value to employees: private data. This data includes medical, payroll and employment information. There is information of value to the company: proprietary data. This includes for example, business plans, manufacturing capabilities, financial data and delivery schedules. It is the computer processing and telecommunication of this data and information which is of major concern to us here today. We will not discuss the protection of classified military information as defined by the Department of Defense.

As a company which operates in a multi-state environment, we have used, for both voice and data transmission, the telecommunication networks available from various common carriers. Because of the rising costs of commercial telephone services, both local and long distance, and the AT&T divestiture, it was necessary to consider communication alternatives. As a result, we are now implementing a communications plan for a Grumman owned and operated telephone system. In addition, a terrestial microwave system is under construction to link our Long Island plants. The other facilities will be interconnected by a satellite communications system.

Telecommunications have been considered safe. Wire tapping is illegal and for the most part, requires physical access to the communication facilities to be effective. However, most long distance commercial carriers use microwave or satellite channels. The monitoring of these channels is passive, non-intrusive and undetectable. Therefore one must postulate that any long distance telecommunications can be monitored.

Grumman as a corporation has reached the point where all facets of its work are affected by the computer. The engineers design the products on terminals connected by communications lines to computers (See Figure 3). Manufacturing people develop programs to drive numerically controlled cutting machines to produce tools and parts. The work on the floor is scheduled and controlled by computers. The business and financial data, payroll, accounts receivables and inventory systems are all computerized. Its obvious that much information about Grumman products and costs are available from its computers and communications networks. It is fairly evident that if an intruder could get into the system he can dissrupt the operation of the company and the disclosure of this information could adversely affect our competitive position.

There are many different computer networks within the company that are used to solve different types of problems. There are networks of large IBM machines for data base processing, computer aided design and interactive timesharing. We have recently purchased a Cray supercomputer for research and engineering design. There are many mini-computers for software development and an ever increasing number of micro or personal computers.

Each of the elements in the system, from the micro to the super computer and each of the communication links, must be addressed from a security viewpoint because each is a possible entry point which can be used to gain access to valuable information.

Several years ago an unsuccessful attempt to get into the Grumman computer was made by a local High School student using a microcomputer. He called to Washington, D.C. and then connected through Telenet to the Grumman timeshare network. He tried to establish a "logon" using various passwords. His effort was noticed by a Grumman systems analyst monitoring the computer usage. With the aid of the FBI the individual was confronted in his home trying to enter the system. We have taken steps which make it much more difficult.

Security is a balancing act. Our people need access to the computer to do their job. They need access from different locations. The greater the access, the greater the security threat. We have and are doing a number of things to protect our systems and information and we will be glad to tell you about some of them.

First, we established a set of written corporate directives to explain to our people what their responsibilities are. It is important to tell people what they must do and why, and it is equally important to tell them what they must not do.

Our directives have established a corporate policy that communications lines which transmit private or proprietary data out of or between Grumman facilities must be encrypted using equipment which conforms to the National Bureau of Standards Data Encryption Standard (DES) and Federal Standard 1027 and is endorsed by the National Security Agency (NSA).

While on this topic, we would like to point out that we have reviewed our telecommunications plans with NSA's Communication Protection Special Projects Office. They have been extremely helpful to us in recommending improvements to the plan, identifying available endorsed equipment and in preparing procedures for use of the DES equipment.

Our directives also prohibit the connection of personal or microcomputers to our network without proper approval. To date a few employees have asked us for permission, but we know there are others on the network. Unfortunately, it gives the user a lot of capability to enter the system and/or to incrementally copy large volumes of data to easily transportable computer readable media not under corporate control. It is a very serious problem and, no one, not even the security agencies have an adequate control mechanism to prevent this kind of abuse.

To minimize this problem, our directives require that data, the computer systems libraries and programs be adequately protected from unauthorized usage. By this we mean that if a person is not authorized to use the computer, that person is denied access to the system and that if a person is authorized to use the computer, that person can only access that information which they are specifically authorized to use. Furthermore, all accesses to the system and data are to be "logged" and an audit trail maintained. We did a study of the available security products and concluded that for us, ACF2, developed by SKK Inc.*, was best suited for use on our large IBM systems. This security product is being phased in over a two year period. Similar security features are inherent in the Control Data furnished operating systems and have been in use for many years on our Control Data Cyber computers.

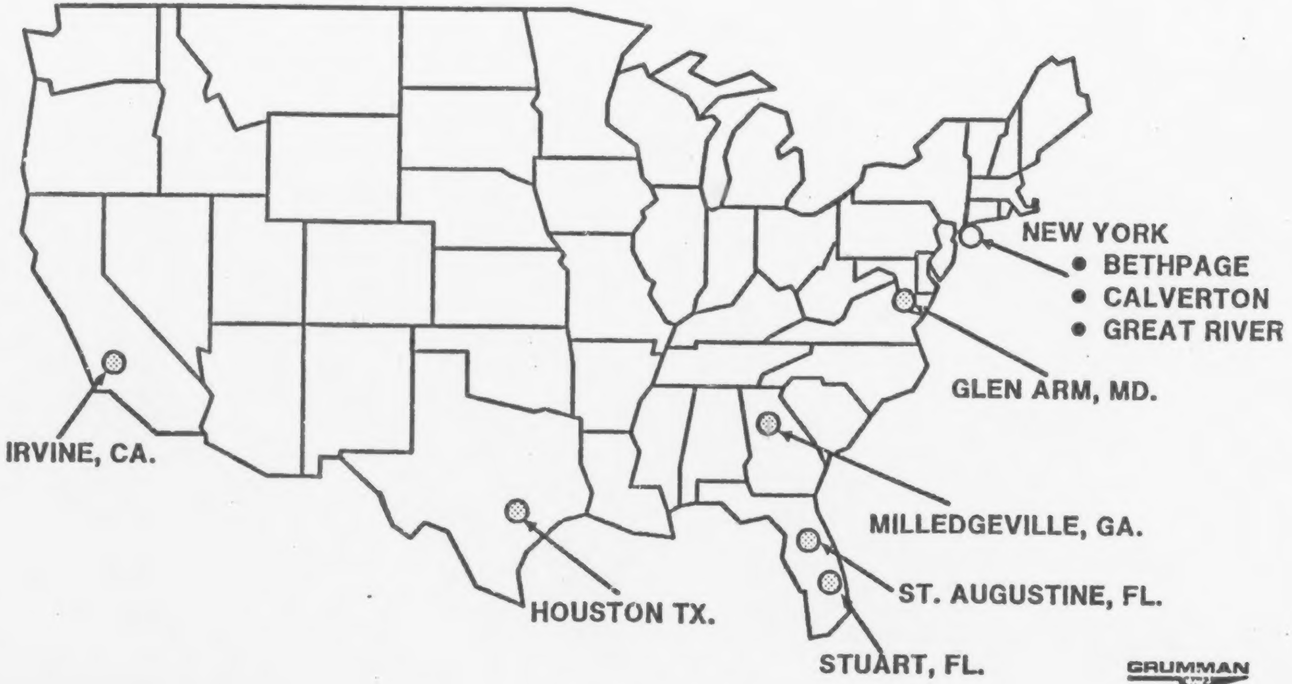
*Schrager Klemens and Krueger, Ltd.

The cost of security is not trivial. At a time when our computing costs are under review and scrutiny by our primary customer, we are making a substantial financial commitment to security. For example, we expect that the protection of the telecommunications network by encryption will cost about $1,000,000 for hardware alone. Similarly, the full implementation of ACF2 requires about 10 dedicated data processing staff years of effort and considerable involvement by the user community. But each of those activities must be accomplished, especially in today's telecommunications and computer dependent environment.

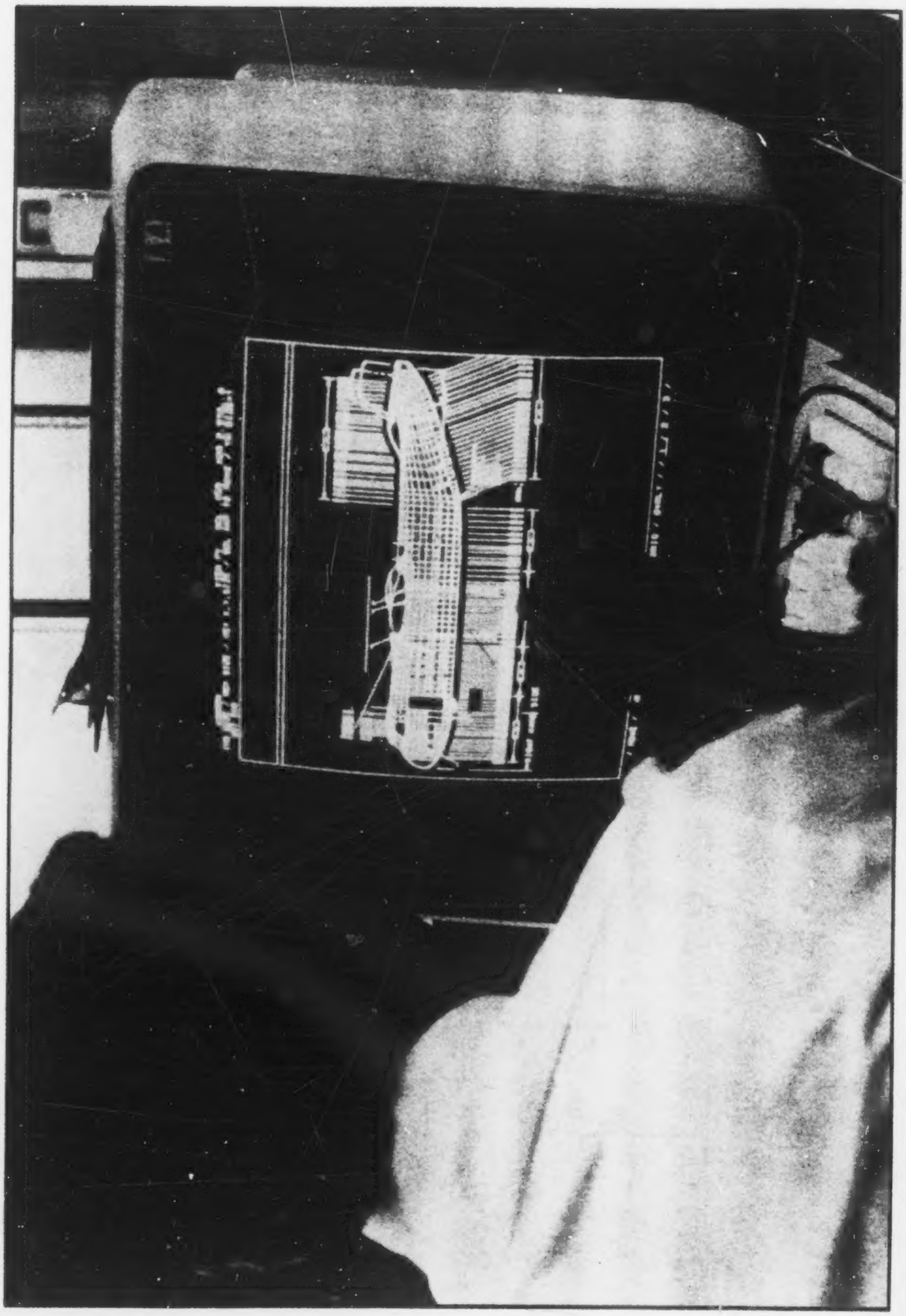
We believe we are doing a good job and are not complacent. We would have to admit that if someone is determined to break in or violate our security, and if they have enough knowledge and resources, they probably can do so. However, we are making it very difficult for them.

GRUMMAN AEROSPACE MANUFACTURING FACILITIES
— BETHPAGE, N.Y.

GRUMMAN AEROSPACE LOCATIONS


NEW YORK
• BETHPAGE
• CALVERTON
• GREAT RIVER
GLEN ARM, MD.
MILLEDGEVILLE, GA.
ST. AUGUSTINE, FL.
STUART, FL.
HOUSTON TX.
IRVINE, CA.

GRUMMAN



Mr. GLICKMAN. The last paragraph of your testimony is one that causes me some concern. You say, "We have to admit that if someone is determined to break in or violate our security, and if they have enough knowledge and resources, they probably can do so. However, we are making it very difficult for them."

I guess my point is that, is it possible to prevent unauthorized access if—the givens of your thing, the conditional part of your sentence is "if they have enough knowledge and resources" may imply that maybe you have to be an insider and be somebody who is trying to destroy the system from the inside. But I guess that sentence causes me some concern, and I wonder if you might amplify on that.

Mr. COHEN. All right. We use commercially available software and computers and, therefore, people who understand the workings and the operations, for example, of large IBM mainframes and most of the operating software there recognize that.

In addition to that, we also use protective software, which again are commercially available. If somebody has made a really exacting study of that, all right, and what he becomes a person which I would classify as dangerous in that if he has access to the system or can get in, he can do things. And there are ways—what man has created man can also uncreate, and there is always that problem.

Mr. GLICKMAN. I think that that is a theme that probably is going to be one that will be a foundation of this subcommittee's—any reports that we make, is that——

Mr. COHEN. One of the things I would like to mention is—you mentioned it with the previous speaker. We do use a tiger team.

Mr. GLICKMAN. Yes.

Mr. COHEN. And this is a small group of people from within the company and sometimes with outside consultants. We don't like to speak about this because their operations are sort of subrosa and from time to time they do go into the system to find our weak spots. OK? Sometimes they have been successful; others they haven't. It's a continual vigilance that we have to do. There are very few people in the company that are aware of their operation.

Mr. GLICKMAN. In using these tiger teams, I mean, are you involved in some cases of interfering with the privacy of your own employees?

Mr. COHEN. No. The only thing the tiger team is allowed to do is to gain access to a data base or a library and leave there an indication that they did access it. They are not allowed to do anything else. They are also under the direction of a trusted Grumman employee to make sure that this thing operates in that fashion.

Mr. GLICKMAN. Are you aware of the term "logic bomb," where you can put something into a computer to take effect later on upon some other condition or some other happening or at some point in time?

Mr. COHEN. I am aware of that. In our experience so far, we have not run across that.

Mr. GLICKMAN. OK. Do you have a classification system whereby you protect unclassified but still sensitive private or proprietary information?

Mr. COHEN. As I said before, we have corporate directives which define what our private data, what our proprietary data, who in the company can classify private data, who in the company can classify proprietary data, who can access it.

The third part of sensitive data, we as a contractor with the Department of Defense are in a—a never, neverland here, I might say. The Department of Defense has set up what they call unclassified national security-related information. This does not come under the general security regime, and yet it also is data which we have to protect, so we do have on their basis a protection of that data.

Mr. GLICKMAN. Do you have employees that have access to Grumman computers and data bases from terminals in their homes?

Mr. COHEN. Yes. As a policy, the company will issue a portable computer to individuals who wish to work flexible hours to work from their home. There are certain conditions they have to abide by.

No. 1, their method of access is to data which is on a machine which is—which has data which is not proprietary nor is it personal data. They strictly are going into a machine which is unclassified and which is not considered to have any protection necessary. This is our time share system, and they are allowed to use that. Now, even to get on that there are protections to make sure that the people know who is coming in and log them on.

Mr. GLICKMAN. And have you had any problems with that situation?

Mr. COHEN. That system was the system where the intruder several years ago tried to get into.

Mr. GLICKMAN. And you were able to catch that individual?

Mr. COHEN. We were able to catch that. We do change our passwords on a regular basis to make sure that they are not passed around.

Mr. GLICKMAN. Have you had any interaction with the DOD Computer Security Center at NSA, for example, in establishing a multilevel company proprietary system or anything else, for that matter?

Mr. COHEN. At the present we are in the process of making contact with them on that particular problem. We are working through the Department of the Navy, which is prime cognizance effort, and we hope to work with them in the near future.

Mr. GLICKMAN. OK. The final question is, where do you think Government can be helpful to you? You alluded to this in your statement. Is it research? Is it computer crime? Is it some GSA directive? Where would you suggest.

Mr. COHEN. I would guess the thing that we would like to stress here is that we would like additional help on how to protect with the use of the microcomputer in our networks and how to protect that from being a tool for intrusion rather than a tool for utility. We have worked with the SA—NSA Special Projects Office. They have been very helpful. We think that continuing working with them we might get some results in this area.

Mr. GLICKMAN. OK, Mr. Cohen. We appreciate very much your testimony today.

Mr. COHEN. Thank you.

Mr. GLICKMAN. Our next witness is Mr. Robert Morris with the Bell Laboratories of the AT&T system. If you do that well, we will give you a job here. [Laughter.]

It is a pleasure to have you here, Mr. Morris, and as I said before, you may feel free to summarize, if you wish.

STATEMENT OF ROBERT MORRIS, TECHNICAL STAFF, BELL TELEPHONE LABORATORIES, AMERICAN TELEPHONE & TELEGRAPH CO.

Mr. MORRIS. Thank you, Mr. Chairman.

I—the written statement that was provided represents not only my personal views but also represents the position of Bell Telephone Laboratories. I will assume that that's been available and has been read, so I will summarize, expand, and add stress where I feel it's appropriate.

The notion that we are raising a generation of children so technically sophisticated that they can outwit the best efforts of the security specialists of America's largest corporations and of the military is utter nonsense. I wish it were true. That would bode well for the technological future of the country.

The fact of the matter is that the technological content of the highly publicized incidents of the last few months, and indeed of the last 2 or 3 years, is really the moral equivalent of joy riding. These kids appear to be having fun and, in most cases, the techniques involved, the techniques required have almost no sophistication whatever. They are the moral equivalent of stealing a car for joy riding purposes when the keys have been left in the ignition.

I don't mean to say it is minor, it is not, because these activities and the fact that these activities can take place have serious implications for the real problems, which I feel are elsewhere.

The accessibility to unauthorized outsiders of computer systems in this country have potential effects on corporate profits, corporate profitability, on individual privacy and on national security, which I think are all extremely important and deserve a great deal of attention, and we have serious concerns in all of these areas.

Bell Laboratories has an immense investment in the whole range of our business: In computers, in computer software, and in computer hardware. Over half of our employees are directly involved in the production of computer software for one system or another, and virtually all of the remaining technical employees have some intimate contact with computers and computerization on a day-by-day business, so that we have a huge investment, both in computers, in computer software, and in the use of computers simply to run our business. The computers contain proprietary information, financial information and, in some cases, because we are a military contractor, military information.

We have a diverse collection of interconnections to our computers and between our computers. We use both the public telephone network and private lines and internal cables within our buildings to connect our employees to our computers, to connect computers one to another, and, indeed, in many cases we not only have to connect employees from one computer to another from diverse locations, but also there are many employees who have terminals at their homes on a regular basis and access the company computers from their homes. So, the networks are large in number and diverse in nature.

We have a number of levels of information that deserve an appropriate level of protection. At the low end are—though still deserving of protection—are electronic mail and the miscellaneous technical information, the documentation, for example, having to do with the progress of a project, of a development project, or general research information that needs to have very wide access to our employees in general; that is, groups work together, experts and consultants are called in and, in many cases, work takes place over very many locations, including from home.

For example, in the preparation of the testimony I am giving, four people are directly involved in the writing, the preparation, the proofreading, and the final production of that testimony.

It was work done in part, either written or proofread from three physically different locations, separated by as much as 20 or 30 miles, and all of the communications and the mail having to do with the status of it, its proofreading, its delivery to this committee, took place by means of electronic mail. This is one example of the pervasive effect of computerization on ordinary business.

Because of the requirement for a relatively broad and easy access—we want to make it easy for our employees to gain access to this technical information—the extent of protection cannot be great. We cannot, for example, restrict this information to require people's physical presence at a computer location. That would simply slow down our business and make our business much more expensive.

A second category of information which requires a higher degree of information is proprietary information, which—whose disclosure would be distinctly injurious to our business. An example would be an unfiled patent or information that leads to an unfiled patent.

Business—corporate plans, marketing plans, that kind of information is kept on a collection of computers with substantially higher security associated with them. That kind of information, for example, cannot be accessed by an employee at a home. You could not generally be accessed by simply dialing a telephone number.

A third category is the information relating to the finances of the company, the personnel records, payroll files, medical information, and sensitive military information.

To get access to information of that category, it cannot be accessed from outside the premises of the company. It would require either a breach of trust—that is, an employee who had the authorization to enter the premises in the particular offices inside the premises, but also a breach of trust while he was in there—or a definitive act of burglary or armed attack.

I have a letter of authorization from a high officer of Bell Laboratories authorizing me, for example, to attempt to act as a tiger team and access some of the personnel and financial records of the company under the agreement that I don't make any modification but simply inform the company of the cases in which I have been able to get access.

And I have been doing this work on a relatively low level, very much part time, over a period of 2 or 3 years, and the judgment that I could make at this point is that I cannot—I have not been able to access, for example, the payroll records of the company without either an egregious breach of trust or an act that would be strictly burglary; that is, breaking down a door or something of that sort.

Even in those cases where I have found it possible to access the information, generally speaking these records are, I have found, impossible to change. It is my judgment at this point, for example, that I could not go to the financial computers of Bell Laboratories and change my annual salary. Even if the file were to be changed, the change would not take effect because of other separate and outside safeguards that are taken.

Now what we have done in the area of computer security, first of all, our computers have a level of physical protection. They are all on our premises, and in most cases the computers themselves are contained within inner offices that require some combination or key or additional authorization to enter.

We have administrative procedures that apply throughout the company. A committee was appointed and met for a period of several years to develop these procedures. The procedures are now in place and have been for well over a year, and they outline the responsibilities of each technical employee for the protection of computer stored information.

We, of course, have not only done original research and development but also have put into place many of the procedures that other witnesses have testified having to do with access control, the preservation of audit traces on who has had access to our computers and what they have looked at.

We have done a certain amount of work in civilian cryptography, and the policies within the company have been set. Each computer within the company—and we have something of the order of 2,000 host computers within the company and tens of thousands of computer terminals capable of accessing those computers—each system has a responsible system administration. He—and it is with him that the buck stops for seeing to it that with the computer that he is supervising the company policies are being met.

Now, we have not been immune to computer intrusion. Intrusions have taken place; many that we have detected, undoubtedly many that we have not detected. We have an assets protection organization which has over the last 2 or 3 years considerably upgraded their skills in detecting and uncovering intruders relatively effectively and rapidly, so that the situation at Bell Laboratories has changed over the past 2 or 3 years where my judgment as of perhaps 1978 or 1979 would be that if one were to dial into our computers and correctly guess a password, the risk of detection and being followed up would have been very small.

The risk now of certainly repeated attempts to intrude onto our computers or in the case where some damage was done or the area was so sensitive that it involved information we felt was highly proprietary, the risk of actually getting caught is considerably improved. We have, in many cases, gotten the cooperation of local police, of the telephone company to trace calls and, in several cases, of the FBI to successfully detect and take appropriate actions against intruders.

In that area, one thing that I would personally very much like to see happen is a much more precise definition of the status of mere computer intrusion in those cases where no harm was intended, and in the vast majority of cases of intrusion that we have encountered no harm was in fact done. Someone—and it is very typically a high school student—was simply having fun.

It is not at all clear at this point whether mere intrusion into a computer system, whether in an intrastate or interstate situation, is or is not a criminal activity. I would very much welcome a clearer definition, such as we have for the interception of communications, where the statutory situation, though quite mixed, is perfectly clear I think to anyone who is likely to take on a civil or criminal responsibility.

Very important to us is risk assessment. As I mentioned in my statement, you do not take the same grade and level of care with protecting the firewood in your woodshed as you do with the currency in your bank vault, and we cannot possibly as a business afford to lay on very complex methods of cryptography and of time consuming access control, such as call-back procedures, for the ordinary, day-to-day technical conduct of our business.

Physical protection is very high on the list of what's required to achieve computer security. Second to that is the indoctrination of personnel into the correct attitudes to preserve computer security. Employees must be educated and, more particularly, management—high management must be convinced of the need for this. If management is not convinced, in general we find that nothing will happen.

It has to a very large extent already occurred in my organization. Management has been convinced, and it's been made perfectly clear to employees what their responsibilities are. Each employee at the company must sign a statement that he has read and understands and will follow the security requirements of the employer, and each new employee, as he comes on, does sign such a statement. And it simply points out to each employee what his own personal portion of the security responsibility is.

We have, in addition, a regular and continuing system of security audits. There is a designated organization within Bell Laboratories that on a regular basis visits each technical computer installation and makes a survey of the security emplacements that exist on that system, what strengths there are, what weaknesses need to be corrected, and the organization that has been audited is required to respond within some period of time, saying what has been done to improve the situation if it were found during the audit.

We have hit teams of two sorts. There are a number of employees whose task is at least in part to simply keep up with the state of the art of computer security, to be aware of the techniques that are being used by intruders and other worse types, and to find out, explore what Bell Laboratories' situation is and what research and development might be required to improve the situation. I don't view our situation with respect to computer security to be particularly comfortable, but that is partly because we are applying rather high standards.

I think that the real problem that is much more important than the casual kind of intrusion that we have seen in the newspapers is that we have to be concerned about much more serious crimes that follow on past this intrusion.

Theft, for example, is common enough and much more common than meets the eye because there are so many cases in which cases of theft from financial institutions and general businesses go unreported to the civil authorities and are, in fact, not prosecuted.

An extremely important and growing area is the theft of proprietary information, and we at Bell Laboratories are extremely sensitive about potential thefts of proprietary information because that information and its preservation goes to the very heart of our continued conduct of our business.

We really only can continue to do business effectively and profitably if we can continue a very strong process of innovation, and if our innovations are short circuited to the outside world before we have been able to get copyright or patent protection or to finish development projects, then we as a business are in very bad shape.

A third area that can be extremely serious is disruption of service. And there is nothing special, of course, about our own particular situation here because the entire fabric of U.S. commerce and U.S. industry is so dependent now on computerization that damage done by outsiders can disrupt almost any kind of service that you can mention, from the running of oil refineries to airlines to communications, transportation, movement of goods.

I would like to go back again to what I said at the beginning. The techniques that we are seeing in recent events are in fact relatively trivial. The opening few minutes of the movie "War Games" was relatively realistic in that what it showed was a very realistic method by which one might gain access to a computer system by seeing the password concealed in a desk. In some cases you find cases where they are posted on the wall, for example, the notion that you can get access to a computer just by dialing numbers and seeing what happens. This sort of thing is real and really does happen.

In general, I think the protection against that kind of intrusion, the technical requirements are already very much in place and what has to be done really is for people to take the security business sufficiently serious that they put in place the obvious and minor steps that are necessary to protect against that. In effect, I think that it would be helpful to—by publicity or by legislation or by whatever persuasive means—to persuade people not to leave the keys in the ignition, and this will solve a very large part of the problem.

I think it would be extremely helpful to define the criminality of the incidents of intrusion where no theft or damage was intended and none was done, and the areas that could be compared with these intrusions are interception of communications.

Thank you.

[The prepared statement of Mr. Morris follows:]

PREPARED STATEMENT OF ROBERT MORRIS

My name is Robert Morris. I am a computer scientist at AT&T Bell Laboratories, and have spent most of my 20-year career there in computer research -- including computer design, computer security, cryptography and related areas.

I am happy to have this opportunity to comment on computer security within the broad context of our experience at Bell Laboratories, and I hope my observations will be useful in your examination of this complex subject.

Computer security is a timely concern and one of growing importance to the U. S. Computer break-ins are familiar now to the general public through news coverage of actual events and through fictionalized events in movies like War Games. Often, the distinction between fact and fiction gets fuzzy. So it's especially reassuring to see this subcommittee probing the complexities and nuances of the issue of computer security.

As a computer scientist at AT&T Bell Laboratories, I will give you, first, a perspective on the extensive computer environment at a large -- but not atypical -- research and development facility. Second, I will briefly define the nature and scope of the basic issue of computer security. Third, I will describe our own concerns about computer security -- which should be representative of other large R&D companies -- and discuss general ways of addressing such concerns. And, finally, I will examine some broad approaches to solutions to the security problem.

At Bell Labs, we are heavily involved with computers and software. About half of our employees now work in software development or support -- compared to about 15 percent in 1974. Today, we have 1800 host computers and a larger number of computer terminals than technical employees. We support about 35 million lines of live code in the Bell System. So that probably makes us one of the biggest software enterprises in the world.

Our computer environment includes centralized computer centers at our various locations. These typically employ large mainframe computers and/or large minicomputers. In addition, there are a number of departmental computers, usually mini's, and professional workstations, usually microcomputers, used by our technical employees.

These computers are interconnected in various ways. For example, we have a network using private lines for high-speed computer-to-computer communications among our locations. In addition, technical employees can use other types of network arrangements to communicate with various computers necessary to their work. Where appropriate, we do use dial-up connections over the nationwide telecommunications network. And a number of employees can also access our computers working via terminals at home.

A major reason for our concern with computer security is that it is possible, at least conceptually, for foreign agents, competitors, hackers -- virtually anyone -- to attempt to gain information from computers that are linked to the telecommunications network.

As we learned how to produce large software systems efficiently and assure the quality of software products, we also established effective software management methods. These include designing in security approaches such as access controls and auditing capabilities to prevent, as well as detect, unauthorized access attempts. We made these methods available and applicable to all parts of Bell Labs. And we have a company-wide Committee on Software Issues to coordinate and standardize our knowledge and procedures.

In general, threats to computer security range from what might be called "simple electronic intrusion" to other forms, including violation of trust by authorized personnel, physical intrusion, persistent espionage by expert agents, and tapping communication lines. My focus will be mainly on simple electronic intrusion because, as various news accounts and our own experience indicate, it is perhaps the most pervasive threat today to computer security. By doing this, however, I do not want to give the impression that the other forms of security threats are not important. Probably the most worrisome of these is violation of trust by authorized personnel -- a problem that, by nature, unfortunately has little to do with the technology of computer security.

Computer security covers both physical security and logical security. The former is enforced by locked doors, guards, and similar types of precautions; the latter, by passwords, file permissions, audits, and the like. I plan to focus on logical security -- including computers, networks and associated software, users, and administrators.

Our goal in computer security at Bell Labs is to strike a balance between security and ease of communication. There is no question that the greater the security, the more limited and difficult the communication. Because technological innovation is at the core of our entire corporate mission, communication is vital -- and this includes communication across boundaries of organizations, technical disciplines, and physical locations.

Implicit here is an obvious, but sometimes overlooked, characteristic of computer security. Just as bank vaults are more heavily secured than the doors of woodsheds, computer security should correspond to the value of the information involved. There should be a multilevel security system -- ranging from minimum to medium to maximum -- keyed to necessary levels of document protection. At Bell Labs, for example, sensitive personnel information such as payroll data is totally isolated from other kinds of information. And access to sensitive data is very tightly controlled.

Another important point about computer security concerns the nature of what we are trying to protect -- electronic information. Someone can steal it without physically removing it from a computer file. This characteristic complicates the job of determining that a theft has, in fact, even taken place. And it also complicates the associated moral and ethical issues.

Finally, a company's top executives must be strongly committed to computer security. Otherwise, there is a real danger that little effective action will be taken. At Bell Labs, for example, we have a company-wide Committee on Software Issues, which I just mentioned. The committee convened a Computer Security Task Force to assess our overall security and make recommendations for improvements, where needed. That task force reported its findings to our entire top management team, which authorized various followup actions. We also have a permanent Security Committee with established policies for our computer centers, and we have computer-security experts in our Assets Protection organization.

Having said all this, let me add that we at Bell Labs have not been immune to electronic intrusion in our less secure computer systems. Our Assets Protection experts are experienced in tracking down electronic intruders. And we have also obtained help, when necessary, from law-enforcement agencies, both local and federal. As a result of this, along with other types of steps I will outline, we are now uncovering intruders much more often and quickly than we used to.

I do not want to imply, however, that the problem of electronic intrusion has totally disappeared -- for us or for any large high-technology company I know of. Electronic intrusion is similar in this respect to the problem of shoplifting faced by retail establishments: Good management and security procedures can contain -- and even minimize -- the problem, but not eliminate it.

Bell Labs concerns about computer security are fairly basic: We want to protect valuable information from theft, alteration, and destruction when it is stored in computer files or transmitted over data lines; we want to prevent unauthorized use of our computer time and resources; and we want to assure a high level of security awareness among both our computer users and administrators. Overall, we want to maintain a consistent, cohesive set of administrative controls for our entire computing environment -- covering hardware, software, and the people involved.

The most important and obvious place to start with computer security is with the people involved, the users and administrators -- as well as their supervisors. The biggest threat to security is carelessness -- for example, logging in to use a computer and then leaving the terminal unattended; sharing passwords for computer access; putting sensitive material into inappropriate computer files.

To summarize some major aspects of our approach to computer security, let me share the following checklist we disseminated for supervisors to assess how computer-secure their organizations are:

- o Do you know who has access to your computers? Don't share passwords -- even with your support staff. If people in your group need access to other employees' files, they should have their own passwords.
- o Does your system refuse unauthorized remote computer requests? If not, this should be remedied by readjusting the permission setting on the computer.
- o Do you have a system administrator? Is it part of his or her job description to monitor and correct security arrangements? The safest systems are those with strong administration.
- o Do you keep private information such as company plans or personnel assessments in your computer files? Assume the worst -- that even a casual browser can read what you enter -- and keep sensitive material elsewhere.

- Do members of your group take computer security seriously? Make sure the employees in your group understand the need for computer security and what they can do to ensure it.

Let's examine a few of these points a bit further -- passwords, for example. In addition to the precaution of "one person, one password," we can increase computer security by using more complex passwords. Computer users all too often have used their first names -- even spouses' or pet names -- or birthdays. In password-cracking, unfortunately, a machine can quickly run down a list of first names or the 20,000 most common words in the English language, as well as all possible birthdays. A more complex alternative might be a password of six characters, which contains both digits and letters. Such a password would be extremely hard to break. Finally, passwords must not be "for all time." They must be changed with some frequency, ideally determined by the desired level of system security.

Another point worth stressing here is the importance of accountability, defined for all involved with the computer system -- user, administrator, and supervisor. For example, all uses of computers require authorization by supervision in order to assign management responsibility to control by whom and for what purposes machines are used. To this end, every machine should have a list of authorized users. In addition -- and of even broader use -- would be a company directory of computers with dial-up access, including identification of organizations associated with particular computers, phone numbers, system administrators, and cognizant management.

A final point to stress in this checklist on computer security is the use of special software packages to increase security by limiting general access to the files of individual users. We can protect information in computer files by using software that limits access to a particular file to its creator, until that person explicitly grants access to others. Another way of limiting access, too, is through hardware that intercepts access attempts, asks for and checks passwords, and calls back authorized users at numbers listed in a directory.

In addition, other software security packages can also track suspected unauthorized attempts at access -- for instance, repeated attempts at logging in or requests for someone else's file. Obviously, we also can limit the number of attempts at logging in or place a time limit on the attempts, after which the connection would automatically be severed.

Technology already exists to provide a high level of computer security. For instance, I am fully confident of the controls on our own computers operating under military security. And I would add that it is prohibitively expensive to break the security controls of most computers that contain classified information. But the penalty of maintaining such a high level of security, of course, is usually isolation of the computers and difficulty of physical entry.

Future progress in the technology of security might well help reduce this penalty -- i.e., by making the overall security controls a bit more transparent to legitimate users. In effect, I am saying that -- just as we are working to make the computers we develop more "user friendly" -- we need to keep these same human needs in mind as we develop or enhance computer security systems.

Technology to deter and detect computer penetration over communications lines could be as simple as a system that identifies calling numbers. This capability could permit security checks against lists of authorized phone numbers. It could also provide records to track down unauthorized access attempts. This identification capability exists within some of today's computerized business communications systems, but is limited to those company lines served by the systems. But the capability is spreading within the nationwide telecommunications network.

In addition, there are possibilities for what we might call "credit-card terminals" -- cheap, tamper-proof means of achieving a much higher level of certainty in identifying users than today's passwords offer. Station identification hardware would also help. This is simply hardware to produce signals that cannot be forged by software, that would improve the level of security in network addresses.

Perhaps the most basic approach to computer security, however, is through people -- as I indicated earlier in a different context. We need what amounts to a national effort at raising people's consciousness of computer security -- and specifically of the moral and ethical implications of attempting to break it. Our education system at all levels can do much to help here. For starters, we need to "deglamorize" computer hackers. They are closer to electronic Peeping Toms, trespassers, and burglars than the popular folk heroes some have made them into. We need to clarify the subtle issues involved in breaking computer security so that no one can claim ignorance of wrong-doing as a defense for such acts.

And let's not forget their victims, either. We also must increase awareness of computer security among those who possess the electronic information. As with physical intrusion and burglary, people who neglect to "lock their doors" share some of the responsibility for any damage or theft of their information.

BIOGRAPHY

Robert Morris

Robert Morris is a computer scientist in the Military Systems Division at AT&T Bell Laboratories in Whippany, New Jersey.

Mr. Morris joined Bell Laboratories in 1960 and has been involved for over twenty years in research and consulting in the computer and communications security areas. During that time he has worked on and made numerous contributions to the security aspects of a large number of AT&T projects. He has received several patents and has authored a number of papers related to computer security and cryptography.

Currently, Mr. Morris is a consultant to the Air Force Studies Board of the National Research Council on the subject of multilevel secure database systems. He also serves in a consulting capacity to the National Security Agency with respect to civilian cryptography.

Mr. Morris received the A.B. and A.M. degrees in mathematics from Harvard University in 1957 and 1958, respectively.

10/83

Mr. GLICKMAN. Have you had any interaction with the DOD Computer Security Center at NSA, for example, in establishing a multilevel company proprietary system?

Mr. MORRIS. Yes, sir, I have. I know most of the—all of the senior staff at the evaluation group. We have worked together with them. I have served on joint committees with members of that group, primarily in governmental and, in particular, in the development of multilevel secure military systems. And we are jointly aware of our problems. We do not have any direct consulting contact with them from a corporate point of view as yet, but that's largely because it's a new organization.

We look forward to working and have worked both with the National Bureau of Standards and with the Computer Security Evaluation Group for the development, particularly of multi-level secure systems where we would like to have relatively insensitive and highly sensitive information resident on the same computer and provide the required separation.

Mr. GLICKMAN. OK.

As communication networks become internationalized, do you see significant additional problems in dealing with security and privacy than we have right now?

Mr. MORRIS. Yes, sir, I do. I don't think that the technical problems will become major in scope, nor, as a matter of fact, are there likely to be new technical problems other than simply the question of international protocols.

What I do see is a complex and growing legal situation because of the barriers that have been and are being erected across national lines to the transport of data. And I think that it is quite likely that we will find ourselves in transporting data internationally burdened by a very diverse set of regulations on that transport of data.

Mr. GLICKMAN. My final question relates to the breakup of the AT&T and the Bell System. Do you think that the proliferation of companies engaged in the manufacture and transmission of communications systems makes it more difficult to provide computer security and privacy?

Most people use phone lines as their access, and if we've got MCI's lines, which are—or GTE's lines or a whole assortment of companies who are involved in communication, not just the Bell System, how do you see that as it relates to what we are talking about today, or does it relate at all?

Mr. MORRIS. It relates only in part. I think that the provision of merely the communications lines is not the largest part of the issue. The more important issues would have to do with the terminal equipment, the computer terminals which amount to the modern telephone from the point of view of data.

We will no longer have only one or a very small number of suppliers who would set standards for such equipment. Much of the equipment, of course, being used now is manufactured overseas, and there are a very large number of companies applying such equipment.

And here I would hope for the possibility of the setting of standards, which is well within the province of the Bureau of Standards, for example, and in military affairs within the province of the DOD computer security group, to provide manufacturers with a set of standards that would be helpful in providing computer security.

Mr. GLICKMAN. OK. We thank you very much for your testimony today. We appreciate your being here.

Mr. MORRIS. Thank you, sir.

Mr. GLICKMAN. I'd like to recess the committee for about 3 minutes, and then we will get to our last witness, Mr. Clegg, vice president of marketing, Federal Systems Division of Honeywell and just—I will be back in about 3 minutes.

[Recess.]

Mr. GLICKMAN. OK. I appreciate the indulgence of the people in the room.

Our final witness is Mr. Clegg. I think you are accompanied by a James Bolton and a Paul Flaherty.

Mr. CLEGG. Yes, sir. I brought along a little help, just in case it is needed.

Mr. GLICKMAN. OK. We can all use help on occasion.

Mr. CLEGG. Congressman Glickman, we——

Mr. GLICKMAN. We appreciate your being here, and as I said before, your statement's in the record, so you may feel free to summarize it, if it expedites or not, or you can read it, if you wish.

STATEMENT OF ELMER I. CLEGG, VICE PRESIDENT, MARKETING, FEDERAL SYSTEMS DIVISION, HONEYWELL INFORMATION SYSTEMS, INC., ACCOMPANIED BY JAMES I. BOLTON, PROGRAM DIRECTOR, FEDERAL SYSTEMS DIVISION, AND PAUL E. FLAHERTY, DIRECTOR, SOFTWARE ENGINEERING, FEDERAL SYSTEMS DIVISION

Mr. CLEGG. We thank you for the opportunity to make this presentation this morning, and I am going to attempt to excerpt from the testimony so that we don't go through the whole thing.

It's my pleasure to share with you this morning the position of Honeywell Information Systems regarding the broad subject of computer security. Honeywell as a corporation has for many years been a leader in the computer industry in providing capabilities to meet the threats of computer and telecommunication security.

Much publicity has been generated recently on problems which exist in the Government and in industry regarding the protection of computerized information. To understand the problems faced by industry and the Government, it's necessary to look at the complex issues associated with computer security.

Computer security is a multifaceted discipline which requires the use of hardware, software and, most importantly, operational procedures to provide protection of valuable resources. The extent of these mechanisms to be employed depends on the value of the information versus the cost impact of its unauthorized disclosure, as has been touched upon by the previous speakers.

Protection of a computer system requires a complete, four-element program consisting of the elements of, No 1, procedural security; No. 2, physical security; No, 3, communications security; and No. 4, operating systems security.

I will not go through a definition of each of these four elements. They are defined and discussed in the body of my testimony, but I would like to summarize by saying that Honeywell plays a contributing role in all four areas of computer security.

First, we provide a variety of educational workshops to both industry and Government which address the procedural and risk analysis aspects of a complete computer security program. And I think it is worth mentioning that we are active with NBS in the conduct of their semiannual seminars on the subject of security.

Second, Honeywell provides a broad spectrum of physical security products to protect the valuable computer resource.

Third, our work in communications security includes specialized systems, fiber optics, and electromechanical emanations control.

But the area we want to address today is the area of operating systems security, and in that area we feel that Honeywell holds a unique position. Going back to the 1972 Anderson report, which was sponsored by the Air Force, the Honeywell MULTICS computer system was recognized as providing the most secure operating system available on the market at that time.

The MULTICS system, which by the way was originally developed as a joint project with both Bell Labs and MIT, provides a unique combination of hardware and software mechanisms which support a variety of interactive applications.

This system is installed at the Air Force Data Services Center in the Pentagon and provides internal controls which allow users at different security levels simultaneous access to the systems information.

The MULTICS system is also in use at a variety of both industry and Government agencies because of its strong security features and control mechanisms. As a recent extension of the MULTICS capability, Honeywell, working in conjunction with the U.S. Navy, has developed a product which we call SCOMP, S-C-O-M-P, and stands for secure communications processor system.

The SCOMP product has bridged the gap between security research and available standard products. This system was designed and developed to provide additional security assurances through the use of new, yet proven concepts of security kernel, formal program verification and trusted computing base concepts.

The SCOMP system is currently being implemented by the U.S. Army, the U.S. Navy, the Department of Energy, and the MITRE Corp. in projects to manage user access to sensitive data in a variety of communication network environments. This state-of-the-art implementation is the result of a jointly funded government/industry effort to solve a major element of the computer security problem.

The Department of Defense continues to lead the way in the research and development of computer security technology within the Government. The DOD Computer Security Center, with whom we work very closely, has become the focal point in DOD for establishing both system and application security requirements.

Honeywell has supported and continues to support the efforts of the center in the timely evaluation of products and capabilities to support both DOD and other Government agencies.

Both the MULTICS and SCOMP computer systems are currently under evaluation at the center. When combined with physical, procedural, and communication controls, these systems, which are currently available, provide a great measure of protection of user information.

The availability and utilization of these products and products similar from other vendors, as well as future advances, is dependent on the clear definition of user security requirements, a point which we feel is lacking very much today.

It's obvious that many of today's Government computer system procurements have vaguely stated security requirements which reflect the complexity and a lack of understanding of the problem of the state of the art. Many times the requirement for computer security, even though thought of in the initial stages of a system specification, is removed prior to requests for vendor offers.

The result of the situation is twofold. First, the implementation of systems and networks embodying greater vulnerability than necessary and, second, the lack of stimulus and incentive for industry focus on enhanced security product development.

In the commercial arena, the major security threat has over the years traditionally been perceived to be from within the company, such as the disgruntled employee. However, recently security requirements in the commercial market are growing rapidly because of the large number of terminal devices and personal computers being employed and available to the general public. These PC's and terminals give malicious users, particularly, the capability to access systems and data not well protected.

In summary, many computer penetrations could be avoided today by applying currently available techniques. The access to computers must be controlled by the use of certifiable user identification and authentication, by automated audit trails, and by other available techniques.

The advances in operating systems security and communications security can also be used as efficient deterrents to computer criminals. I must again stress that it is imperative that the requirement for computer security be clearly understood and stated in the procurement process, whether the buyer is a Government agency or an industrial concern.

Technological developments can and will continue to improve the available state of the art if the marketplace encourages it, but only if that encouragement comes. Realistic objectives and milestones must be established and timely recognition of achievement of these objectives must be awarded in and through the procurement process.

The state of the art in both penetration methods and security methods, as pointed out earlier, is not static. An advance in one will normally be offset by an advance in the other.

Finally, recognition and definition of computer requirements in the design phase of a system is critical, especially in the areas of communication security and operating systems security. Security mechanisms of these types are difficult to achieve as add-ons to an existing system. The initial specification must contain certain characteristics to provide this capability and, therefore, must become more important in the procurement process.

I have indicated today that Honeywell recognizes the complexity of the broad subject of computer security. We have been heavily involved in all aspects of computer security, and we will continue to provide systems and solutions to meet unique security requirements in both Government and industry.

Mr. Chairman, this concludes my statement. We thank you for the opportunity, and we would be happy to respond to any questions.

[The prepared statement of Mr. Clegg follows:]

STATEMENT OF ELMER I. CLEGG

It is my pleasure, and my privilege, to share with you this morning the position and philosophy of Honeywell Information Systems regarding computer security. For over a quarter of a century, Honeywell has been a leader in the computer industry in providing capabilities to meet many of the threats to computer and telecommunications security. Your invitation to us requested our views on any or all of the following:

1) Current and future threats and vulnerabilities to our Information/communications technology dependent society;
2) the scope of telecommunications security research efforts in the computer vendor industry;
3) other efforts in the private sector at improving computer security;
4) the appropriate role of Federal agencies in providing computer security direction, specifically policy formulation, resource allocation, and ordering priorities.

My testimony will focus on items (3) and (4) above.

A great deal of publicity has been generated recently documenting problems which exist in government and industry regarding the protection of computerized information. To understand the problems faced by industry and the Government, it is necessary to look at the complex issues associated with computer security.

Computer security is a multi-faceted discipline which requires the use of hardware, software, and operational procedures to provide protection of valuable resources. The extent of these mechanisms depends on the value of the information versus the cost of its unauthorized disclosure.

The question that must be answered, relative to the extent of computer security, is what is the risk or threat being addressed by the application of computer security techniques. If the protection mechanism makes the cost of obtaining the information exceed the value of the information, the computer security threat has been eliminated. The identification of the risk associated with a perceived threat is often easier to identify in a Government setting than in industry. The risk is often a breach of privacy regarding sensitive information pertaining to individuals, groups, or corporations and obviously the disclosure of information pertaining to national security issues. In industry the threat may be financial, a loss of real property, or technology, or loss of market position, or product innovations.

Protection of a computer system requires a complete program of 1) Procedural Security, 2) Physical Security, 3) Communications Security and 4) Operating Systems Security.

Procedural Security requires formal methods for controlling access to classified or sensitive information. These protection methods are often the enforcement of regulation, as in the Department of Defense, or of audit principles as in industry.

Physical Security addresses the protection within the physical environment of the computer facility. The protection of the computer from physical attack has received a great deal of attention since the 60's when bombing computer centers was a form of protest. Today computers are protected by security systems such as sophisticated burglar/fire alarms, guards, card keys, and other physical protection devices and techniques.

Communications Security is addressed through the use of encryption and protection against electromagnetic emanation from transmission lines. The use of the Data Encryption Standard (DES) and Tempest approved equipment are the most well known methods of providing communications security.

Operating System Security is the system of internal controls in the computer which ensure that all data in the system is protected from unauthorized access or disclosure as well as from tampering. The DoD Computer Security Center has developed criteria which define the features and techniques necessary to provide operating system security at various risk levels.

Honeywell plays a contributing role in all four areas of computer security. We provide a variety of educational workshops to industry and government which address the procedural and risk analysis aspects of a complete computer security program. Honeywell provides a broad spectrum of physical security products to protect the valuable computer resource. Our work in communications security includes specialized systems, fiber optics and electromagnetic emanations control.

In the area of Operating System Security, Honeywell holds a unique position. In the 1972 Anderson report, sponsored by the Air Force, the Honeywell MULTICS Computer System was recognized as the most secure operating system available on the market. The MULTICS system provides a unique combination of hardware and software mechanisms which support a variety of application requirements. This system is installed at the Air Force Data Services Center in the Pentagon and provides the user community internal controls which allow users at different security levels access to MULTICS simultaneously. The MULTICS system is in use at a variety of industry and Government agencies because of its strong security features and control mechanisms.

As an extension of the MULTICS capability, Honeywell in conjunction with the Navy, has developed the Secure Communications Processor (SCOMP) System. The SCOMP product has bridged the gap between computer security research and available standard products. SCOMP applies many of the MULTICS concepts in a mini computer system. The system was designed and developed to provide additional security assurances through the use of the security kernel, formal program verification and Trusted Computing Base Concepts. The SCOMP system is currently being implemented by the U. S. Army, U. S. Navy, Department of Energy and the MITRE Corporation in projects to manage user access to sensitive data in a variety of communication network environments.

This state-of-the-art implementation is the result of a Government/industry effort to solve a major element of the computer security problem.

The Department of Defense continues to lead the way in the research and development of computer security technology. The DoD Computer Security Center has become the focal point in DoD for establishing system and application security requirements. Honeywell has supported and continues to support the efforts of the center in the timely evaluation of products and capabilities to support

DoD and other government agenices. SCOMP is currently under evaluation at the Center. When combined with physical, procedural and communications controls, these currently available computer systems provide complete protection of user information.

The availability and utilization of these products and future advances is dependent on the clear definition of user security requirements. Many of today's Government procurements have vaguely stated security requirements which reflect the complexity and a lack of understanding of the problem or the state-of-the-art. Many times the requirement for computer security is removed prior to request for vendor offers. The result of this situation is the implementation of systems and networks embodying greater vulnerability than necessary and the lack of qualified stimulus and incentive for industry focus on enhanced security product development.

In the commercial arena, the major security threat has been perceived to be from within (i.e., the disgruntled employee). However, security requirements in the commercial market are growing rapidly because of the large number of terminal devices and personal computers available to the general public. These PC's and terminals give malicious users the capability to access systems and data not well protected.

Many computer penetrations could be avoided by applying currently available techniques. The access to computers must be controlled by the use of "certifiable" user identification and authentication; by automated audit trails; and by other available techniques. The advances in Operating System Security and Communications Security can also be used as efficient deterents to computer criminals. I must again stress that it is imperative that the requirements for computer security are clearly understood and stated in the procurement process. Technological developments can and will continue to improve the available state-of-the-art if the marketplace encourages it. Realistic objectives and milestones must be established and timely recognition of achievement of these objectives rewarded in the procurement process. The state-of-the-art in both penetration methods and security mechanisms is not static. An advance in one will normally result in an advance in the other.

Finally, recognition and definition of computer requirements in the design phase of a system is critical, especially in the areas of Communications Security and Operating Systems Security. Security mechanisms of these types are difficult to achieve as an "add-on" to an existing system. The initial design must contain certain characteristics to provide this capability and therefore must become more important in the procurement process. I have indicated today that Honeywell recognizes the complexity of computer security. We have been heavily involved in all aspects of computer security and will continue to provide systems and solutions to meet unique security requirements in both Government and industry.

Mr. Chairman, this concludes my formal statement. We will be happy to respond to any questions the Committee may have.

Mr. GLICKMAN. Thank you very much, Mr. Clegg.

I think that as far as I am concerned one of the most significant things in your statement is on page 6, when you talk about the Government's procurements have "vaguely stated security requirements" and "many times the requirement for computer security is removed prior to request for vendor offers." This all results in greater vulnerability and lack of attention. I think this is stated even much more clearly than was kind of implicitly stated in some of our previous testimony.

I wonder if you might give us any suggestions on what the Government ought to do. Should OMB take it more seriously? Should—as was stated by Dr. Ware, maybe GSA should come out with a handbook, so to speak, that should be applied across the board?

Mr. CLEGG. Well, I have never been much of a fan of the actual utility of things like handbooks. I don't see that they would hurt, but I can't see that they're going to result in major progress in the attack on the problem.

I would agree with Dr. Ware, however, that we are, in essence, playing a game of catch-up here. As an example, we were in the development of the SCOMP product quite a bit before the DOD Computer Security Center came into existence. And since the time that it did come into existence, we have worked very closely with the center in the—in the further development of that product and specification of it and implementation of the product.

But, of course, the arrival on the scene by the organization caused some disruptions and some redirection of our efforts. In the long run, I think the formation of the Computer Security Center is a very large step and a very necessary one in the forwarding of the work in that field.

Perhaps——

Mr. GLICKMAN. What about a national commission that's been talked about before? Do you think that would be helpful?

Mr. CLEGG. Yes, I do. I think, as one of the other people advocated, that such a commission, I believe, needs to look at the subject of computer security on two different planes and that you cannot just lump together the needs of the highest levels of security concern in the Department of Defense with the concern in industrial corporations.

There is a risk tradeoff that has to be made, which is a very practical tradeoff. How valuable is the information you have? What is the cost that you will incur? What is the cost impact if that information—the security of that information—is breached? In an industrial concern that is a major tradeoff question that has to be addressed.

Mr. GLICKMAN. Let me just ask you a final question.

You've developed some systems that have gotten NSA's scrutiny. I wonder if you might describe how your interactions with the National Bureau of Standards and NSA have helped you in the development of security systems for the private sector.

Mr. CLEGG. Why don't I let Mr. Bolton answer that question, since he's a little more involved in the development and interaction with NSA.

Mr. GLICKMAN. OK.

Mr. BOLTON. I think, as Mr. Clegg pointed out, the thing that both groups have done have provided a focal point for the exchange of ideas and information. In the case of NSA, they are in the process of establishing standards and criteria to which private enterprise can certify security mechanisms. That certification process then would make available to anyone with that kind of a problem a set of guidelines against which he could measure his requirements and, therefore, make the cost tradeoff risks that we've talked about.

Mr. GLICKMAN. And it obviously has provided some help to you on some specific systems that you have been involved in?

Mr. BOLTON. Yes.

Mr. CLEGG. It certainly has.

Mr. GLICKMAN. Mr. McCandless.

Mr. MCCANDLESS. Please forgive my lack of sophistication, but in what areas are you concentrating? What technology are you applying to the security aspect of this? Codes? Deciphers? Box keys?

Mr. CLEGG. It is a combination of both computer hardware and software capabilities which employ all of the things that you have mentioned.

Mr. FLAHERTY. Keys and codes are add-on security features. We are building the security from within the operating system of the computer, employing both hardware and software techniques to provide for security. Those keys and codes are something you add on later, once you have the data to transmit the data.

Mr. CLEGG. Mr. McCandless, at least two of the previous speakers have talked about the use of standard available commercial operating systems and software on their computer systems. The products that we have talked about are products that are specifically designed for computer applications in a security environment and, therefore, this ties into my statements about the need—if the Government or industry specifies their security needs in a computer procurement, these kinds of products can be phased in through the initial design and specification of those systems. Adding them on to an existing situation is much more difficult than introducing them in the systems design phase, but they do make use of all of the things that we have talked about.

Mr. **McCandless**. Well, of course, your company is one of the major producers of computers. From what your testimony has said, you are specializing in this area. Are you working on the add-on aspect of it or are you saying that when you are a prime bidder, you ought to be able to have this as a part of that request for proposals, that the security system be included? What thrust are we at here this morning?

Mr. **Clegg**. Well, I—let me just say this. We feel it is much better to address this in the systems specification and design phase. That's point No. 1.

In real life, we have a multitude of industrial concerns and Government agencies using computers, and we feel that the best place where our technology can be employed in ongoing situations is in the area of telecommunications networking, and that is the interfacing of one computer system with another, the interfacing of a variety of terminals and work stations with main frame or large computers, and the type of security hardware—computer security hardware—we are talking about can be employed very well in the phased implementation of those kinds of networks which are taking place today, so they do have application in the ongoing.

Mr. **McCandless**. Your company has specialized in another field, and that is in environmental monitoring of large office buildings and so forth, where central computers give necessary information to cut the cost of heating, cooling, maintenance, operation of the building.

I am trying to place together here, there is still the one thing—in other words, I can't buy, is what you are telling me, a black or a brown or a blue box that is built by Honeywell and put it on my IBM or contract with you to provide some kind of a third-party security system or something like that. What you are talking about is the actual hardware application of your product and building into that the original——

Mr. **Clegg**. Integrated. It is integrated as part of the computer system; yes.

Mr. **McCandless**. So you are not—you don't have any boxes that you are selling, then?

Mr. **Clegg**. Well, I wish it were that simple. Let me tell you a couple of things that we are doing.

Our Building Controls Division, which—which has responsibility for designing the commercial systems which do all the things of environmental and related controls that you talked about, are—is now being driven much more by a communications and computer order of discipline than they have in the past and the integration of the computer and communications capability into the building controls systems is happening today and building systems are being designed with those kinds of things built into them.

So, we are working to integrate the computer security capabilities into the other parts of the corporate efforts as well. I would just say that in summary to your--to your questions that I think that the computer hardware that we are talking about, hardware and software systems, which are particularly focused on the field of computer security, have application either in the building of a new system or in the tying together of existing systems.

That is a facet I think that puts us in very good stead in the competitive marketplace, but it's an area where there has not been tremendous, certainly, I think quantitatively very little encouragement on the part of either industry or the Government to develop complete systems and products to attack this problem, which is another point that I've tried to make in the testimony. I think that there needs to be more emphasis on the part of the Government in encouraging industry to be active in this field.

Mr. **McCandless**. Is the cipher/decipher system something that is still in the future or are you working on that in a practical basis?

Mr. **Clegg**. The cipher/decipher system in the field of communications security?

Mr. **McCandless**. Right.

Mr. **Clegg**. Well, it is something that is practical today but it is something that is quite costly today, as one of the previous speakers pointed out, and the application of it in industry, as we've heard, is taking place in some fields, such as the financial community, but the broad application of it in industry is not yet really taking place.

Mr. **McCandless**. Thank you, Mr. Clegg.

Thank you, Mr. Chairman.

Mr. **Glickman**. Thank you.

Just one final question. What's the level of interest among your customers in the private sector in computer communications security? What protection do they say they need, and has the level of increase—level of interest increased lately?

Mr. **Clegg**. The level of increase has—the level has increased dramatically in the recent past, and I think that it is a recognition of the extent of the threat and the dispersion of personal computers and intelligent terminals into homes, into small offices, as well as all levels of industrial concern and Government agencies, has brought the focus on the threat. I predict that over the next 3 years that this will be an area of great concern on the part of industry, but over the last decade it certainly hasn't because the threat has not been there.

Mr. **Glickman**. OK. Well, we thank you for your excellent testimony today. This will conclude the hearings.

I would like to say before we leave today a special note of recognition to Louise Becker at the Library of Congress, who helped us establish the format for these hearings and who is well known throughout the country as one of the experts in the area. Without her I don't think that we could have put together the most comprehensive set of hearings on the subject I think that have ever been held by the U.S. Congress.

I am sure that we will be preparing a committee report which will outline the testimony, together with perhaps making some recommendations—maybe not legislative, we haven't talked about that yet—but at least some recommendations about where we can go vis-a-vis the U.S. Government's role and all of—all of the issues that we are talking about today.

The hearing stands adjourned.

[Whereupon, at 12:05 p.m., the subcommittee was adjourned.]

APPENDIX

Statement Submitted for the Record by IBM Corp.

Much is currently being written and reported in the media about the explosive growth and change in information processing. The rapid assimilation of computing capability and telecommunications into a broad spectrum of public and private applications has made, what was a specialty area a decade ago, a household word today. With the technological changes that are emerging from the many arenas of information systems development...hardware, software, telecommunications...fundamental changes are also coming in the number and nature of users, their environments and how they use computers. Up until now, the use of the hundreds of thousands of installed computers were the domain of the expert. But not for much longer.

For example, several industry estimates suggest that with the advent of the personal computer, intelligent workstations and terminals, and efficient and user-friendly applications software, there will be, by the mid-eighties, more information systems users who are not expert in technical systems aspects than those who are. Armed with little more than a word processing or spread-sheet package and the appropriate hardware, hundreds of thousands of non-expert computer users have joined the ranks of the technical specialists users. Computers are found on desktops, in hostile work environments, in vehicles, in classrooms, in just about any situation where people can find use for information.

It is, therefore, not surprising that with these dramatic changes in the use of information systems, equally significant changes should also be required in information systems security. We would like to present some of these considerations to the committee for its assessment along with a report on some of the techniques, both technological and procedural, which we consider necessary to deal with these new security and audit requirements.

Throughout this paper, we will concentrate on the principle that the integrity of the information itself is the primary objective, second only to the protection of the persons involved. Protection of devices or environments while important in themselves, is a means to an end. As the cost of computing and telecommunications devices continues to drop, more and more decisions relating to physical security will be governed not by the asset value of the equipment itself but by the value of the information stored or processed therein. This represents a change of some significance from previous thinking...a change made possible by technological advances and market conditions.

Information security threats are generally categorized by the industry:

1. Errors and Omissions
2. Dishonest Employees
3. Disgruntled Employees
4. Fire
5. Water
6. External Break-in and Attack

While there is less agreement on the absolute dimensions of each of these categories, most experts agree that this list does represent a priority sequence in which more potential damage can develop from the authorized individuals who make up the first three classes than from physical or external sources.

Several conclusions can be drawn from that analysis. The first is that the primary arena for protective efforts is within the information-using organization. The second and less obvious conclusion is that on examination, many of the techniques used to protect against the first three threats also have salutary effects in dealing with the external break-in and attack.

Three additional points should be mentioned. The first point is that today an information system should be described as a highly interdependent combination of people, equipment and telecommunications facilities bound together by software, policies and procedures. The purpose of the system, of course, is to support the information requirements of the using organization. We recommend that in all assessments this interdependence and breadth of involvement be kept in mind. Each facet of the system...people, equipment, telecommunications, software, procedures...all contribute to the integrity of the system and conversely to its weaknesses. Concentrating on any single aspect or on all of the aspects individually misses the important points of interrelation...the so-called interfaces...-where vulnerabilities are more prone to exist. At the points where user meets equipment, where equipment meets equipment, where organizational responsibilities change, the possibilities for different priorities, levels of security commitment and different understanding of security requirements also exist.

The second point is that system management and security are inextricably bound together. Security programs that are organizationally isolated from the information functions are operating at a significant disadvantage. However, in today's environment, the information functions themselves are moving back into the operating and management segments of the organization. Data processing departments are increasingly becoming custodians and suppliers of the resources with less and less direct ownership of the information or the application process. The obvious conclusion is that as information ownership and control diffuses itself through an organization, the responsibility for security goes with it. Therefore, the major constituency for security awareness and responsibility today is the user and owner. Designating the rules of usage and the degree of control is the duty of the individual or organization which owns the information. Quite often these are not information processing specialists.

The third point is that security is achieved by a combination of functions, some of which are preventive in nature and some of which are designed for detection. The industry cannot overestimate the value of a well managed and fully supported audit program as a deterrent. Even if total prevention is out of the question because of technical, economic or operational considerations, detection if it is understood by all parties as being effective, can make a major contribution toward discouraging misuse of information systems.

For its part, IBM understands that there is a significant security contribution to be made by information system suppliers. IBM has a formal and longstanding corporate policy concerning our customers' information security. (A copy of that policy letter is attached). As part of that commitment, we offer training programs and hundreds of security and audit publications, as well as films and videotapes to assist our customers and the public to better understand and implement appropriate security and audit programs. (Sample material is attached.)

In addition, we regard it as part of our responsibility to make available hardware and software technology to enable our customers to increase their information protection capability. Through systems for access control and personal identification, techniques for encrypting information, integrity of system design, audit and control tools, clarity and ease of use to help reduce errors and omissions, we are trying to ensure that technological protection keeps pace with technological advances in speed, capacity and function. But technology cannot do it all and that is why we also put so much emphasis and resource into customer awareness and training as we do.

In today's environment, the challenge is to supply security function as part of the overall information management system. Because of the broad variation in the nature and value of the information which may be processed and stored on the same class or type of hardware and software, it is necessary to offer security function as a series of options to be selectively applied by the user as required. Security functions imposed by the manufacturer stand the risk of being inappropriate and in some cases may actually create problems by inducing frustration and increased error rates on the part of the user.

Levels of security will vary and one of the most fundamental requirements for any security system to be a success is a classification scheme which identifies the information asset by its value to the organization and its susceptibility to compromise, misuse or destruction. This is sometimes called Risk Assessment. The classification scheme must then outline what steps must be taken not just to protect the information in computing systems but wherever it is. Mail procedures, conversation, document storage, electronic storage, modification, audit trail are all subjects of this scheme. Only with a clear and realistically implementable classification program in place can a truly effective security program be carried out. (A sample risk assessment form is attached.)

We see our obligation to continue to provide improved methods of prevention and detection as well as to continue to supply our customers with the information they require to help develop their own security programs. For their part, we believe that they must provide the policy and the means of implementing that policy...-resources, management, assessment and enforcement across the entire spectrum of information usage.

MEMORIAL SLOAN-KETTERING CANCER CENTER

Radhe Mohan, Ph.D., Head
Medical Physics Computer Service

The computer that was affected at Memorial Sloan-Kettering Cancer Center is the one used for recording and verifying treatments of our radiation therapy patients and for the Memorial Dose Distribution Service which provides radiation therapists in 80 hospitals across the country with calculations of appropriate radiation doses for their respective patients.

The following is the sequence of events of the break-in and subsequent identification of the intruders.

On the morning of June 3, when the Medical Physics Computer systems manager, Mr. Chen Chui, arrived at work, he discovered that the computer identified above had failed for a short period of time during the night. In investigating the cause, Mr. Chui discovered an unauthorized entry had been made, and he took the steps which would usually be sufficient to block further entry. The New York City police were immediately notified.

On June 7, another unauthorized entry into the computer system was made. Further investigation led to the discovery that the intruder had created a way to regain entry. While the intruder was using the computer, we were able to communicate with him by computer mail, and he telephoned us. We asked him to stop trying to enter our system and requested that he tell us how he broke into the computer originally. Rather than take the chance that he would succeed in breaking into the system again and cause problems, we provided him with a special account which he could use safely, if he insisted on accessing our computer. The police and telephone company were consulted on this.

The major reason for entry into this special account area was to allow the telephone company to trace the calls being made in an attempt to catch the intruder(s). When they persisted in calling, the telephone lines were tapped by the police and the area from which the calls were being made was discovered.

In no way did any of the tampering affect the treatment of patients receiving radiation therapy. Only the accounting information -- billing records to the 80 hospitals -- was affected. After four weeks of monitoring, all necessary adjustments were made and the system continues to operate effectively as it did during the period of monitoring.

○